

## PATENT COOPERATION TREATY

PCT

NOTIFICATION OF RECEIPT OF  
RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira  
No.11 Mori Building  
6-4, Toranomom 2-chome  
Minato-ku  
Tokyo 105-0001  
JAPON

Date of mailing (day/month/year) 13 September 2000 (13.09.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference SK00PCT75	International application No. PCT/JP00/05543

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

SONY CORPORATION (for all designated States except US)  
ASANO, Tomoyuki et al (for US)

International filing date : 18 August 2000 (18.08.00)  
Priority date(s) claimed : 20 August 1999 (20.08.99)  
21 December 1999 (21.12.99)  
Date of receipt of the record copy by the International Bureau : 04 September 2000 (04.09.00)  
List of designated Offices :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE  
National : JP, US


## ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase  
☒ confirmation of precautionary designations  
☐ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer:  Shinji IGARASHI Telephone No. (41-22) 338.83.38
--	--

**THIS PAGE BLANK (USPTO)**

## INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. **It is the applicant's responsibility** to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

**For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.**

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

## CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

## REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

**THIS PAGE BLANK (USPTO)**



## PARENT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING  
SUBMISSION OR TRANSMITTAL  
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira  
No.11 Mori Building  
6-4, Toranomom 2-chome  
Minato-ku  
Tokyo 105-0001  
JAPON

Date of mailing (day/month/year) 13 September 2000 (13.09.00)	
Applicant's or agent's file reference SK00PCT75	IMPORTANT NOTIFICATION
International application No. PCT/JP00/05543	International filing date (day/month/year) 18 August 2000 (18.08.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 20 August 1999 (20.08.99)
Applicant SONY CORPORATION et al	

- The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
- An asterisk(\*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
20 Augu 1999 (20.08.99)	11/234371	JP	04 Sept 2000 (04.09.00)
21 Dece 1999 (21.12.99)	11/363266	JP	04 Sept 2000 (04.09.00)

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Shinji IGARASHI

Telephone No. (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**

# PATENT COOPERATION TREATY

**PCT**

## NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

KOIKE, Akira  
No.11 Mori Building  
6-4, Toranomom 2-chome  
Minato-ku  
Tokyo 105-0001  
JAPON

Date of mailing (day/month/year) 01 March 2001 (01.03.01)		
Applicant's or agent's file reference SK00PCT75		IMPORTANT NOTICE
International application No. PCT/JP00/05543	International filing date (day/month/year) 18 August 2000 (18.08.00)	Priority date (day/month/year) 20 August 1999 (20.08.99)
Applicant SONY CORPORATION et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

EP,JP

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 01 March 2001 (01.03.01) under No. WO 01/15380

### REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

### REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.


The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---

**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

SK00PCT75

副本 - 印刷日時 2000年08月18日 (18.08.2000) 金曜日 13時43分29秒

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/RO/101 この特許協力条約に基づく国際 出願願書は、 右記によって作成された。	PCT-EASY Version 2.91 (updated 01.07.2000)
0-5	申立て 出願人は、この国際出願が特許 協力条約に従って処理されるこ とを請求する。	
0-6	出願人によって指定された受理 官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	SK00PCT75
I	発明の名称	情報伝達システム及び方法、ドライブ装置及びアクセ ス方法、情報記録媒体、記録媒体製造装置及び方法
II	出願人	出願人である (applicant only)
II-1	この欄に記載した者は	米国を除くすべての指定国 (all designated States except US)
II-2	右の指定国についての出願人で ある。	
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川6丁目7番35号
II-5en	Address:	7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP

**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

SK00PCT75

副本 - 印刷日時 2000年08月18日 (18.08.2000) 金曜日 13時43分29秒

III-1	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor) 米国のみ (US only)  浅野 智之 ASANO, Tomoyuki 141-0001 日本国 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-1	この欄に記載した者は	
III-1-2	右の指定国についての出願人である。	
III-1-4ja	氏名(姓名)	
III-1-4en	Name (LAST, First)	
III-1-5ja	あて名:	
III-1-5en	Address:	
III-1-6	国籍(国名)	日本国 JP
III-1-7	住所(国名)	日本国 JP
III-2	その他の出願人又は発明者	出願人及び発明者である (applicant and inventor) 米国のみ (US only)  大澤 義知 OSAWA, Yoshitomo 141-0001 日本国 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-2-1	この欄に記載した者は	
III-2-2	右の指定国についての出願人である。	
III-2-4ja	氏名(姓名)	
III-2-4en	Name (LAST, First)	
III-2-5ja	あて名:	
III-2-5en	Address:	
III-2-6	国籍(国名)	日本国 JP
III-2-7	住所(国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)  小池 晃 KOIKE, Akira 105-0001 日本国 東京都 港区 虎ノ門二丁目6番4号 第11森ビル No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-1ja	氏名(姓名)	
IV-1-1en	Name (LAST, First)	
IV-1-2ja	あて名:	
IV-1-2en	Address:	
IV-1-3	電話番号	
IV-1-4	ファクシミリ番号	

**THIS PAGE BLANK (USPTO)**



## 特許協力条約に基づく国際出願願書

副本 - 印刷日時 2000年08月18日 (18.08.2000) 金曜日 13時43分29秒

IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)	
IV-2-1ja	氏名	田村 榮一; 伊賀 誠司	
IV-2-1en	Name(s)	TAMURA, Eiichi; IGA, Seiji	
V	国の指定		
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE 及びヨーロッパ特許条約と特許協力条約の締約国である他の国	
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	JP US	
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。		
V-6	指定の確認から除かれる国	なし (NONE)	
VI-1	先の国内出願に基づく優先権主張		
VI-1-1	先の出願日	1999年08月20日 (20.08.1999)	
VI-1-2	先の出願番号	平成 1 1 年特許願第 2 3 4 3 7 1 号	
VI-1-3	国名	日本国 JP	
VI-2	先の国内出願に基づく優先権主張		
VI-2-1	先の出願日	1999年12月21日 (21.12.1999)	
VI-2-2	先の出願番号	平成 1 1 年特許願第 3 6 3 2 6 6 号	
VI-2-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	4	-
VIII-2	明細書	232	-
VIII-3	請求の範囲	35	-
VIII-4	要約	1	absk00pct75.txt
VIII-5	図面	94	-
VIII-7	合計	366	

**THIS PAGE BLANK (USPTO)**

**THIS PAGE BLANK (USPTO)**

## 特許協力条約に基づく国際出願願書

SK00PCT75

副本 - 印刷日時 2000年08月18日 (18.08.2000) 金曜日 13時43分29秒

	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-10	包括委任状の写し	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1, VI-2	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-18	要約書とともに提示する図の番号	1	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	小池 晃	
IX-2	提出者の記名押印		
IX-2-1	氏名(姓名)	田村 榮一	
IX-3	提出者の記名押印		
IX-3-1	氏名(姓名)	伊賀 誠司	

## 受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面:	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であつてその後期間内に提出されたものの実際の受理の日(訂正日)	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

## 国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

**THIS PAGE BLANK (USPTO)**

## 国際調査報告

(法8条、法施行規則第40、41条)  
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 SK00PCT75	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/JP00/05543	国際出願日 (日.月.年) 18.08.00	優先日 (日.月.年) 20.08.99
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。  
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 6 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

## 1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☒ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 1 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

---

**THIS PAGE BLANK (USPTO)**

## 第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (PCT 17 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であって PCT 規則 6.4(a) の第 2 文及び第 3 文の規定に従って記載されていない。

## 第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲 1-117 は、相互認証を行うドライブ装置及び情報記録媒体からなるシステム、あるいは各々の装置、あるいは各々の装置間での情報伝達方法又は情報記録媒体へのアクセス方法に関するものであり、一方、請求の範囲 118-137 は、記録媒体製造装置又は記録媒体製造方法に関するものである。

この両者 (請求の範囲 1-117 の群と請求の範囲 118-137 の群) に共通の事項は、記録媒体及び相互認証のためのセキュリティモジュールを含む情報記録媒体のみであるが、調査の結果、相互認証を行う情報記録媒体は、芳尾太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス、第 739 号、(1999 年 3 月 22 日)、pp. 49-53 に開示されているから、新規でないことが明らかとなった。

結果として、請求の範囲 1-117 の群と請求の範囲 118-137 の群とに共通の事項は、先行技術の域を出ないから、PCT 規則 13.2 の第 2 文の意味において、特別な技術的事項ではない。したがって、上記 2 群の請求項は、発明の単一性を満たしていない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

---

**THIS PAGE BLANK (USPTO)**



## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup>

H04L 9/32 H04L 9/08 G11B 20/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup>H04L 9/00 G09C 1/00-5/00 G11B 20/00 G06K 17/00  
G06F 12/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

INSPEC (WPI)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	芳尾太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, 1999年3月22日号 (Np. 738), pp. 49-53, 特に51頁中欄及び図1参照	1, 2, 6, 7, 34, 35, 37, 64, 65, 67, 69, 91-93, 95
Y		3-5, 21-23, 26-33, 36, 51-53, 56-63, 66, 68, 7 8-80, 83-90, 94, 102- 104, 107-117
A		1-137

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

26. 10. 00

国際調査報告の発送日

07.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政



5 W

9 5 7 0

電話番号 03-3581-1101 内線 3576

---

**THIS PAGE BLANK (USPIC)**

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 10-133953, A (株式会社トキメック) 22. 5月. 1998 (22. 05. 98), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	J P, 5-75598, A (松下電器産業株式会社) 26. 3月. 1993 (26. 03. 93), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	J P, 63-184164, A (横江川 光) 29. 7月. 1988 (29. 07. 88), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
Y	J P, 11-7412, A (株式会社オプトロム) 12. 1月. 1999 (12. 01. 99) &WO, 98/58319, A1 &EP, 919929, A1 &AU, 9880344, A &CN, 1229487, A &TW, 374912, A	3-5, 36, 66, 68, 94
Y	J P, 7-161172, A (ソニー株式会社) 23. 6月. 1995 (23. 06. 95), ファミリーなし	3-5, 36, 66, 68, 94
Y	J P, 11-120679, A (ソニー コーポレーション オブ アメリカ) 30. 4月. 1999 (30. 04. 99), ファミリーなし	3-5, 36, 66, 68, 94
Y	臼木直司, 飯塚裕之, 山田正純, 松崎なつめ “IEEE1394バスの著作権保護方式”, 映像情報メディア学会技術報告, Vol. 22, No. 65, (Nov 1998), pp. 37-42 (CE'98-14), 特に38頁左欄参照	26, 28-30, 32, 56, 58-60, 62, 83, 85-87, 89, 107, 109-111, 113
Y	廣瀬勝一, 吉田進 “安全な認証付Diffie-Hellman鍵共有プロトコル とその会議鍵配布への応用”, 電子情報通信学会技術研究報告, Vol. 97, No. 252, (1997), pp. 87-96 (ISEC97-37)	27, 31, 33, 57, 61, 63, 84, 88, 90, 108, 112, 114
Y	J P, 5-347617, A (株式会社東芝) 27. 12月. 1993 (27. 12. 93), ファミリーなし	27, 31, 33, 57, 61, 63, 84, 88, 90, 108, 112, 114

---

**THIS PAGE BLANK (USPTO)**

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	Rainer A Rueppel and Paul G van Oorschot, "Modern key agreement techniques," computer communications, (Jul 1994); pp. 458-465	115-117 8-25, 38-55, 70-82, 96-106
Y A	Lein Harn and Shoubao Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution," IEEE Journal on Selected Areas in Communications, Vol.11, No.5, (Jun 1993), pp. 757-760	115-117 8-25, 38-55, 70-82, 96-106
Y A	J P, 2-278489, A (株式会社シーエスケイ) 14. 11月. 1990 (13. 11. 90), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y A	J P, 10-187826, A (日本電気株式会社) 21. 7月. 1998 (21. 07. 98), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y A	J P, 7-319967, A (株式会社テック) 8. 12月. 1995 (08. 12. 95), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
A	J P, 11-205305, A (ソニー株式会社) 30. 7月. 1999 (30. 07. 99) &EP, 930556, A2	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137

---

**THIS PAGE BLANK (USPTO)**

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 6-161354, A (日本電信電話株式会社) 7. 6月. 1994 (07. 06. 94) & EP, 856821, A2 & EP, 856822, A2 & US, 5396558, A & US, 5446796, A & US, 5502765, A	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y	Digital Transmission Content Protection Specification, Revision 1.0, (12 Apr 1999), Volume 1 (Informational Version), 特に4.5節及び第7章参照	2, 8-13, 17- 23, 35, 38-43, 47-53, 65, 70- 72, 75-80, 92, 96, 99-104, 115-137

---

**THIS PAGE BLANK (USPTO)**



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L 9/32 H04L 9/08 G11B 20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L 9/00 G09C 1/00-5/00 G11B 20/00 G06K 17/00  
G06F 12/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS)  
INSPEC (WPI)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Taro YOSHIO, "Kogata Memory Card de Ongaku Chosakuken wo mamoru," Nikkei Electronics, 22 March, 1999 (22.03.99) (Np.738), pp.49-53, especially, see page 51, middle column, and Fig. 1	1, 2, 6, 7, 34, 35, 37, 64, 65, 67, 69, 91-93, 95
Y		3-5, 21-23, 26-33, 36, 51-53, 55-63, 66, 68, 78-80, 83-90, 94, 102-104, 107-117
A		1-137
X	JP, 10-133953, A (TOKIMEC INC.), 22 May, 1998 (22.05.98) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	JP, 5-75598, A (Matsushita Electric Ind. Co., Ltd.), 26 March, 1993 (26.03.93) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
26 October, 2000 (26.10.00)Date of mailing of the international search report  
07 November, 2000 (07.11.00)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 63-184164, A (Hikari YOKOEKAWA), 29 July, 1988 (29.07.88) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117
Y	JP, 11-7412, A (Oputoromu K.K.), 12 January, 1999 (12.01.99) & WO, 98/58319, A1 & EP, 919929, A1 & AU, 9880344, A & CN, 1229487, A & TW, 374912, A	3-5, 36, 66, 68, 94
Y	JP, 7-161172, A (Sony Corporation), 23 June, 1995 (23.06.95) (Family: none)	3-5, 36, 66, 68, 94
Y	JP, 11-120679, A (Sony Corporation of America), 30 April, 1999 (30.04.99) (Family: none)	3-5, 36, 66, 68, 94
Y	Naoji USUKI, et al., "IEEE1394 Bus no Chosakuken Hogo Houshiki", Eizou Jouhou Media Gakkai Gijutsu Houkoku, Vol.22, No.65, (Nov 1998), pp.37-42 (CE'98-14), especially, see page 38, left column	26, 28-30, 32, 56 , 58-60, 62, 83, 8 5-87, 89, 107, 10 9-111, 113
Y	Katsuichi HIROSE, et al., "Anzenna Ninshoutsuki Diffie-Hellman Kagi Kyouyuu Protocol to sono Kaigi Kagi Haifueno Ouyou", Technical Research report, the Institute of Electronics, Information and Communication Engineers, Vol.97, No.252, (1997), pp.87-96 (ISEC97-37)	27, 31, 33, 57, 61 , 63, 84, 88, 90, 1 08, 112, 114
Y	JP, 5-347617, A (Toshiba Corporation), 27 December, 1993 (27.12.93) (Family: none)	27, 31, 33, 57, 61 , 63, 84, 88, 90, 1 08, 112, 114
Y	Rainer A Rueppel and Paul G van Oortscot, "Modern key agreement techniques," computer communicatins, (July, 1994), pp.458-465	115-117
A		8-25, 38-55, 70-82, 96-106
Y	Lein Harn and Shoubao Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution," IEEE Journal on Selected Areas in Communications, Vol.11, No.5, (June, 1993), pp.757-760	115-117
A		8-25, 38-55, 70- 82, 96-106
Y	JP, 2-278489, A (CSK Corporation), 14 November, 1990 (14.11.90) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38-50, 54, 55, 70-77, 81-82, 96-101, 105, 106 , 118-137
Y	JP, 10-187826, A (NEC Corporation), 21 July, 1998 (21.07.98) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38- 50, 54, 55, 70-77 , 81, 82, 96-101, 105, 106, 118-13 7

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 7-319967, A (TEC CORPORATION), 08 December, 1995 (08.12.95) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
A	JP, 11-205305, A (Sony Corporation), 30 July, 1999 (30.07.99) & EP, 930556, A2	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
A	JP, 6-161354, A (Nippon Telegr. & Teleph. Corp. <NTT>), 07 June, 1994 (07.06.94) & EP, 856821, A2 & EP, 856822, A2 & US, 5396558, A & US, 5446796, A & US, 5502765, A	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
Y	Digital Transmission Content Protection Specification, Revision 1.0, (12 Apr 1999), Volume 1 (Informational Version), Especially, see Chapter 4, Par. No. 4.5 and Chapter 7	2, 8-13, 17-23, 35, 38-43, 47-53 , 65, 70-72, 75-80, 92, 96, 99-104, 115-137

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

Claims 1 to 117 relate to a system consisting of a drive device and an information recording medium that mutually authenticate each other, or individual devices, or a method of information transmission between individual devices or a method of accessing an information recording medium, while claims 118 to 137 relate to a recording medium production device or a recording medium production method.

Although the both (group of claims 1 to 117 and group of claims 118 to 137) share only a recording medium and an information recording medium including a security module for mutual authenticating, our search result has evidenced that the mutually-authenticating information recording medium is disclosed in "Protecting music copyright by small-sized memory card" by Taro Yoshio, Nikkei Electronics, No. 739 (1999-3-22), pp.49-53, and therefore is not novel.

Accordingly, since the subject matters shared by the group of claims 1 to 117 and the group of claims 118 to 137 are still at a prior-art level, they do not constitute any special technical matters in terms of the second sentence of PCT Rule 13.2. Therefore, the above two groups of claims do not fulfill the requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest



- The additional search fees were accompanied by the applicant's protest.  
No protest accompanied the payment of additional search fees.

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001 年 3 月 1 日 (01.03.2001)

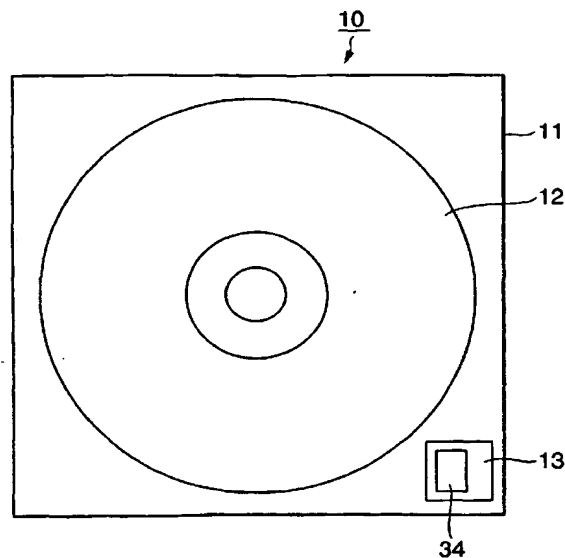
PCT

(10) 国際公開番号  
WO 01/15380 A1

- (51) 国際特許分類<sup>7</sup>: H04L 9/32, 9/08, G11B 20/10 (ASANO, Tomoyuki) [JP/JP]. 大澤 義知 (OSAWA, Yoshitomo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/05543
- (22) 国際出願日: 2000 年 8 月 18 日 (18.08.2000)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:  
特願平 11/234371 1999 年 8 月 20 日 (20.08.1999) JP  
特願平 11/363266 1999 年 12 月 21 日 (21.12.1999) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 浅野智之
- (74) 代理人: 小池 晃, 外 (KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).
- (81) 指定国 (国内): JP, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
- 添付公開書類:  
— 国際調査報告書
- 2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: INFORMATION TRANSMISSION SYSTEM AND METHOD, DRIVE DEVICE AND ACCESS METHOD, INFORMATION RECORDING MEDIUM, DEVICE AND METHOD FOR PRODUCING RECORDING MEDIUM

(54) 発明の名称: 情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法



(57) Abstract: An information recording medium is provided with a security module, data to be recorded on the information recording medium are encrypted using encryption keys different for individual elements of data, and the security module keeps the encryption keys safely. Further, the security module performs a mutual authentication using a drive device and disclosed

[続葉有]

WO 01/15380 A1



---

key encryption techniques, and gives an encryption key to a device after confirming that the device has received an authentic license to thereby prevent the leakage of data to an illegal device. Accordingly, an illegal copying (against the will of a copyright holder) of copyrighted data such as movie and music can be prevented.

(57) 要約:

情報記録媒体にセキュリティモジュールを持たせ、情報記録媒体上に記録されるデータを個々のデータ毎に異なる暗号鍵で暗号化し、暗号鍵をセキュリティモジュールが安全に保管する。また、セキュリティモジュールは、ドライブ装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。これにより、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにする。

## 明細書

情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法

### 技術分野

本発明は、安全にデータを授受することを可能にした情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法に関する。

### 背景技術

近年は、情報をデジタル的に記録する記録装置及び記録媒体が普及しつつある。これらの記録装置及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録装置及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

このような著作権保護のための手法として、例えば、ミニディスク（MD）（商標）システムにおいては、いわゆるSCMS (Serial Copy Management System) と呼ばれる方法が用いられている。当該

S C M S の情報は、デジタルインターフェースによって、音楽データとともに伝送される情報であり、この情報は、音楽データがコピーフリー（以下、copy freeと記す）であるか、又は、1回のみコピーを許す（以下、copy once allowedと記す）データであるか、コピーが禁止されている（以下、copy prohibitedと記す）データであるかのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインターフェースから音楽データを受信した場合、上記S C M S の情報を検出し、これがcopy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、当該S C M S の情報をcopy prohibitedに変更して受信した音楽データとともに記録し、copy freeであれば、当該S C M S の情報をそのまま、受信した音楽データとともに記録する。

このように、ミニディスクシステムにおいては、S C M S の情報を用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、デジタルバーサタイルディスク（Digital Versatile Disk : DVD（商標））システムにおける、コンテンツスクランブルシステムが挙げられる。このシステムでは、ディスク上の著作権を有するデータが全て暗号化され、ライセンスを受けた記録装置だけが暗号鍵を与えられ、これにより上記暗号化されているデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録装置は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされる



のを防いでいる。

しかしながら、上記のミニディスクシステムが採用している方式では、S C M S が copy once allowed であれば、これを copy prohibited に変更し、受信したデータとともに記録するなどの動作規定に従わない記録装置が、不正に製造されてしまう虞がある。

また、上記の D V D システムが採用している方式では、再生のみ可能な R O M メディアに対しては有効であるが、ユーザがデータを記録可能な R A M メディアにおいては有効ではない。すなわち、R A M メディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録装置で動作するディスクを新たに作ることができるからである。

このようなことから、本件出願人は、先に出願した日本特許出願である特願平 1 0 - 2 5 3 1 0 号（日本特許公開平 11-224461:1999 年 8 月 17 日 公 開）の特許出願において、個々の記録媒体を識別するための情報（以下、媒体識別情報と呼ぶ）を記録媒体に持たせ、この情報はライセンスを受けた装置しかアクセスできないようにすることにより、不正コピーを防止する技術を提案している。すなわち、当該技術においては、記録媒体上のデータを、ライセンスを受けることによって得られる秘密に基づく鍵と媒体識別情報の両方を用いて暗号化することにより、ライセンスを受けていない装置がデータを読み出しても意味のないものとしている。さらに、当該技術によれば、装置にライセンスを与える際にその装置の動作を規定し、不正コピーを行わないようにもしている。このように、上記技術によれば、ライセンスを得ていない装置は媒体識別情報にアクセスでき

ず、また媒体識別情報は個々の媒体毎に個別の値になっているため、例えばライセンスを受けていない装置がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないことになり、不正コピーの防止が実現されている。

しかしながら、上記技術においては、ある記録装置によって情報が記録された記録媒体を他の装置にて再生できることを保証するために、記録媒体上のデータを暗号化するための暗号鍵は、システム全体で共通の秘密鍵（Secret Key）（マスターキー）に基づいて生成されるようになっている。これはすなわち、例えば正当な一つの装置が解析されて不正にマスターキーが盗まれてしまうようなことが起きると、そのシステムの任意の装置によって記録されたすべてのデータの暗号が解かれ、システム全体が壊滅する恐れがあることを意味している。

#### 発明の開示

そこで、本発明の目的は、暗号鍵を安全に保管することができるようにした情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

また、本発明の他の目的は、不正な機器にデータを漏らすことのないように、或いは正当な機器のみにデータを供給できるようにした情報伝達システム及び方法、ドライブ装置及びアクセス方法、情

報記録媒体、記録媒体製造装置及び方法を提供することにある。

また、本発明の他の目的は、正当な機器ではあるが、例えば不正な解析により当該機器の秘密が露呈してしまったような場合に、当該機器に対して新たにデータを与えてしまうことをも防ぐことができるようにした、情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

さらに、本発明の他の目的は、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにした情報伝達システム及び方法、ドライブ装置及びアクセス方法、情報記録媒体、記録媒体製造装置及び方法を提供することにある。

本発明では、情報記録媒体にセキュリティモジュールを持たせる。情報記録媒体上に記録されるデータは、個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管する。また、セキュリティモジュールは記録／再生装置と公開鍵暗号技術を用いた相互記証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。さらに、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な機器ではあるが不正な解析によって当該機器の秘密が露呈してしまったような場合に、その装置に新たにデータを与えてしまうことをも防ぐことができるようにする。

すなわち、本発明に係る情報伝達システムは、データを記録する

情報記録媒体と前記情報記録媒体にアクセスするドライブ装置とを有するシステムであり、前記情報記録媒体は、前記ドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、データを記録する記録媒体とを具備し、前記ドライブ装置は、前記情報記録媒体へのアクセス時に相互認証プロトコルを実行する制御部と、前記情報記録媒体の記録媒体にアクセスするインターフェース部とを具備することにより、上述した課題を解決する。

また、本発明の情報伝達方法は、データを記録する記録媒体を備えた情報記録媒体と、前記情報記録媒体にアクセスするドライブ装置との間で情報の伝達を行う際の情報伝達方法であり、前記ドライブ装置が備える制御部と前記情報記録媒体が備えるセキュリティモジュールとの間で相互認証プロトコルを実行し、前記相互認証プロトコルの認証結果に応じて、前記ドライブ装置が前記情報記録媒体の記録媒体へアクセスすることにより、上述した課題を解決する。

次に、本発明のドライブ装置は、データを記録する記録媒体と、ドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールとを具備する情報記録媒体に、アクセスするドライブ装置であって、前記情報記録媒体へのアクセス時に相互認証プロトコルを実行する制御部と、前記情報記録媒体の記録媒体にアクセスするインターフェース部とを具備することにより、上述した課題を解決する。

また、本発明のドライブ方法は、データを記録する記録媒体と、ドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールとを具備する情報記録媒体に、アクセスするドライブ方法であって、前記情報記録媒体へのアクセス時に相互認証プロトコ

ルを実行し、前記相互認証プロトコルの認証結果に応じて、前記情報記録媒体の記録媒体にアクセスすることにより、上述した課題を解決する。

ここで、前記相互認証プロトコルは、公開鍵暗号技術を用いたプロトコルである。前記情報記録媒体は、前記セキュリティモジュールと前記記録媒体であるディスクとを具備し、前記ドライブ装置は、前記情報記録媒体の記録媒体であるディスクを駆動する駆動部を更に具備する。前記情報記録媒体は、前記セキュリティモジュールと前記記録媒体であるメモリチップとを具備する。インターフェース部は、直接、前記記録媒体にアクセスするか又は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスする。

また、前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶しており、前記ドライブ装置は、その内部に自己を識別する為の識別情報を記憶している記憶部を更に具備し、前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記識別情報を交換し、互いに相手の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わない。

前記情報記録媒体の識別情報は、前記セキュリティモジュール内に記憶されており、前記情報記録媒体は、前記リストを前記セキュリティモジュール内に記憶している。前記情報記録媒体は、前記リストを前記記録媒体内に記憶している。前記ドライブ装置は、前記記憶部に前記リストを記憶或いは記憶していない。

前記セキュリティモジュールと前記ドライブ装置の何れか一方若

しくは両方がリストを保持するか否かに応じた相互認証プロトコルを実行する。前記ドライブ装置の制御部は、前記セキュリティモジュールが前記リストを記憶している前記情報記録媒体か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行する。前記情報記録媒体のセキュリティモジュールは、前記リストを記憶している前記ドライブ装置か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行する。

前記情報記録媒体は、その内部に前記リストのバージョン番号及びリストを記憶しており、前記ドライブ装置は、前記記憶部にその内部に前記リストのバージョン番号及びリストを記憶しており、前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、新しいリストを持つ方が、それを他方に送り、古いリストを持つものは送られた新しいリストを用いて自分のリストを更新する。

前記情報記録媒体は、その内部に前記リストのバージョン番号を記憶しており、かつ、前記記録媒体上にリストが記録されており、前記ドライブ装置は、前記記憶部にその内部に前記リストのバージョン番号及びリストを記憶しており、前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、前記ドライブ装置は、自己のリストが新しい場合には、自己のリストを前記情報記録媒体に書き込み、自己のリストが古い場合には、前記情報記録媒体からリストを読み出し、読み出したリストを用いて自分のリストを更新する。

前記ドライブ装置及び前記セキュリティモジュールは、共に上記新しいリストを用いて、相手の識別情報がリストに登録されているか否かを確認する。

前記ドライブ装置は、その内部に自己を識別する為の識別情報を記憶している記憶部を更に具備し、前記情報記録媒体のセキュリティモジュールは、前記相互認証プロトコル処理時に、前記識別情報を前記ドライブ装置から受信し、前記ドライブ装置の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わない。

前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶しており、前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記識別情報を前記セキュリティモジュールから受信し、前記セキュリティモジュールの識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わない。

前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリストであり、このリストに登録されている機器を排除すべき機器とする。前記不正な機器を排除するためのリストは、排除すべきでない機器の識別情報が登録されたリストであり、このリストに登録されていない機器を排除すべき機器とする。前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、

リボケーションリストに登録されている、及び／又は、レジストレーションリストに登録されていない機器を排除すべき機器とする。前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、前記リボケーションリストとレジストレーションリストのうち何れか一方を選択的に、排除すべき機器となっているか否かを判定する。

前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を暗号化して一方から他方に送る。前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化して一方から他方に送る。

前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いて、データを暗号化する暗号鍵を暗号化して前記セキュリティモジュールに送り、前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、前記ドライブ装置は、前記暗号鍵で



暗号化されたデータと前記セキュリティーモジュールによって保存鍵で暗号化された暗号鍵を前記インターフェース部を介して記録媒体に記録する。

前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、前記ドライブ装置と前記セキュリティーモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記ドライブ装置は、暗号化された暗号鍵を前記記録媒体から読出し、前記読み出された暗号鍵を前記セキュリティーモジュールに送り、前記セキュリティーモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を前記セキュリティーモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて、復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティーモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵で暗号化されたデータを前記記録媒体から読み出して復号する。

前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、記ドライブ装置と前記セキュリティーモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いて暗号化した、データを暗号化する暗号鍵と前記暗号鍵を用いて暗号化したデータとを前記セキュリティーモジュールに送り、前記セキュリティーモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を

鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いてを再度暗号化した暗号鍵と、前記ドライブ装置から受信した前記暗号鍵を用いて暗号化したデータとを前記記録媒体に記録する。

前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いてデータを暗号化して前記セキュリティモジュールに送り、前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化されたデータを共有された鍵を用いて復号し、暗号鍵を用いて、復号したデータを暗号化して記録媒体に格納する。

前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記セキュリティモジュールは、暗号化された暗号鍵と前記暗号鍵を用いて暗号化されたデータとを前記記録媒体から読出し、前記暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて再度暗号化した暗号鍵と前記記録媒体から読み出した暗号鍵で暗号化されたデータを前記ドライブ装置に送り、前記ドライブ

装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵を用いて、暗号化されたデータを復号する。

前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、前記セキュリティモジュールは、暗号化されて情報記録媒体に格納されているデータを読み出すと共に、暗号鍵を用いて暗号化されたデータを復号し、前記鍵共有プロトコルによって共有した鍵を用いて、復号されたデータを再度暗号化してドライブ装置に送り、前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化されたデータを復号する。

次に、本発明の情報記録媒体は、データを記録する記録領域を有する情報記録媒体であり、外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールと、データを記録する前記記録領域を有する記録媒体とを具備することにより、上述した課題を解決する。

また、本発明のアクセス方法は、データを記録する記録領域を有する情報記録媒体のアクセス方法であり、外部装置と接続し、乱数を生成して前記外部装置に送信し、前記外部装置から受信した情報

と保存している情報とを使用して、前記外部装置との間で公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行い、前記外部装置との間で相互認証プロトコルを実行し、前記相互認証プロトコルの認証結果に応じて、データを記録するための記録媒体にアクセスすることにより、上述した課題を解決する。

ここで、上記セキュリティモジュールは、データを記録する前記記録媒体にアクセスするためのインターフェース機能を更に具備する。

次に、本発明の記録媒体製造装置は、情報記録媒体を製造する記録媒体製造装置であって、記録媒体にアクセスするドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、データを記録する記録媒体とを具備する情報記録媒体に、不正な機器を排除する処理に用いられるリストを記録する記録部を具備することにより、上述した課題を解決する。

また、本発明の記録媒体製造方法は、情報記録媒体を製造する記録媒体製造方法であって、記録媒体にアクセスするドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、データを記録する記録媒体とを具備する情報記録媒体に、不正な機器を排除する処理に用いられるリストを記録することにより、上述した課題を解決する。

ここで、前記セキュリティモジュールと前記記録媒体とを有する前記情報記録媒体を組み立てる組立部を更に具備する。

前記記録部は、前記セキュリティモジュール内に前記リストを記録する。前記記録部は、前記リストのバージョン番号及び前記リストを前記セキュリティモジュール内に記録する。前記記録部は、

前記記録媒体上に前記リストを記録する。前記記録部は、前記リストのバージョン番号を前記セキュリティーモジュール内に記録し、前記リストを前記記録媒体上に記録する。前記記録部は、前記情報記録媒体の識別情報、前記情報記録媒体に与えられた公開鍵暗号技術で用いられるプライベート鍵及びパブリック鍵証明書、前記リストのバージョン番号を前記セキュリティーモジュール内に記録する。

前記記録部が前記情報記録媒体に記録する前記リストを格納する格納手段を更に具備する。前記記録部が前記情報記録媒体に記録する前記リストを外部から入手するインターフェースを更に具備する。

前記リストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び／又は排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されている。

#### 図面の簡単な説明

図 1 は、本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティーモジュールを有する光ディスク情報記録媒体の構成を示す図である。

図 2 は、光ディスク情報記録媒体のセキュリティーモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティーモジュールの一例を示すブロック図である。

図 3 は、本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えた光ディスク記録再生装置の構成を示すブロック図である。

図 4 は、パブリック鍵証明書の説明に用いる図である。

図5は、リボケーションリストを説明するための図である。

図6は、第1の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図7は、第1の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図8は、第1の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図9は、第1の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図10は、第1の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図11は、第1の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図12は、本発明を適用した実施の形態としてリスト格納用の不揮発性メモリを備えたセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

図13は、メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えたセキュリティモジュールの一例を示すブロック図である。

図14は、本発明を適用した実施の形態のメモリ記録再生装置の構成を示すブロック図である。

図15は、第2の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図16は、第2の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 1 7 は、第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図 1 8 は、第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

図 1 9 は、第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 2 0 は、第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図 2 1 は、第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図 2 2 は、第 2 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

図 2 3 は、レジストレーションリストを説明するための図である。

図 2 4 は、第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 2 5 は、第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 2 6 は、第 3 の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図 2 7 は、第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 2 8 は、第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図 2 9 は、第 3 の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図 3 0 は、第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 3 1 は、第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 3 2 は、第 4 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図 3 3 は、第 2 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

図 3 4 は、第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 3 5 は、第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図 3 6 は、第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図 3 7 は、第 4 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

図 3 8 は、リボケーションリスト／レジストレーションリストを説明するための図である。

図 3 9 は、第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 4 0 は、第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 4 1 は、第 5 の実施の形態の光ディスク情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図 4 2 は、第 5 の実施の形態の光ディスク情報記録媒体からデー



タを再生する際の基本的な処理手順の内容を示す図である。

図 4 3 は、第 5 の実施の形態の光ディスク情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図 4 4 は、第 5 の実施の形態の光ディスク情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図 4 5 は、第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 4 6 は、第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 4 7 は、第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際の他の例の処理手順の内容を示す図である。

図 4 8 は、第 6 の実施の形態のメモリ情報記録媒体にデータを記録する際のさらに他の例の処理手順の内容を示す図である。

図 4 9 は、第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 5 0 は、第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の詳細な処理手順の内容を示す図である。

図 5 1 は、第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際の他の例の処理手順の内容を示す図である。

図 5 2 は、第 6 の実施の形態のメモリ情報記録媒体からデータを再生する際のさらに他の例の処理手順の内容を示す図である。

図 5 3 は、リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有する光ディスク情報記録媒体の構成を示す図である。

図 5 4 は、光ディスク情報記録媒体のセキュリティモジュールで

あって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

図55は、リスト格納用の不揮発性メモリを備えないセキュリティモジュールを有するメモリ情報記録媒体の構成を示す図である。

図56は、メモリ情報記録媒体のセキュリティモジュールであって、リスト格納用の不揮発性メモリを備えないセキュリティモジュールの一例を示すブロック図である。

図57は、第7の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

図58は、第7の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図59は、第7の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図60は、第7の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図61は、第8の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

図62は、第8の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図63は、第8の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図64は、第8の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図65は、第9の実施の形態の光ディスク情報記録媒体とその光ディスク記録再生装置の構成を示すブロック図である。

図 6 6 は、第 9 の実施の形態の光ディスク情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 6 7 は、第 9 の実施の形態の光ディスク情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 6 8 は、第 9 の実施の形態の光ディスク情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 6 9 は、第 1 0 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

図 7 0 は、第 1 0 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 7 1 は、第 1 0 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 7 2 は、第 1 0 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 7 3 は、第 1 1 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

図 7 4 は、第 1 1 の実施の形態のメモリ情報記録媒体にデータを記録する際の基本的な処理手順の内容を示す図である。

図 7 5 は、第 1 1 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 7 6 は、第 1 1 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 7 7 は、第 1 2 の実施の形態のメモリ情報記録媒体とそのメモリ記録再生装置の構成を示すブロック図である。

図 7 8 は、第 1 2 の実施の形態のメモリ情報記録媒体にデータを

記録する際の基本的な処理手順の内容を示す図である。

図 7 9 は、第 1 2 の実施の形態のメモリ情報記録媒体にデータを記録する際の詳細な処理手順の内容を示す図である。

図 8 0 は、第 1 2 の実施の形態のメモリ情報記録媒体からデータを再生する際の基本的な処理手順の内容を示す図である。

図 8 1 は、メディアタイプ I M 1 に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

図 8 2 は、メディアタイプ I M 2 に相当する光ディスク情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

図 8 3 は、メディアタイプ I M 3 に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

図 8 4 は、メディアタイプ I M 4 に相当するメモリ情報記録媒体のセキュリティモジュールにおける処理の流れを示すフローチャートである。

図 8 5 は、デバイスタイプ D e v 1 及び D e v 3 の記録再生装置の処理の流れを示すフローチャートである。

図 8 6 は、デバイスタイプ D e v 2 及び D e v 4 の記録再生装置の処理の前半部分の流れを示すフローチャートである。

図 8 7 は、デバイスタイプ D e v 2 及び D e v 4 の記録再生装置の処理の後半部分の流れを示すフローチャートである。

図 8 8 は、メディアタイプ I M 1 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロッ

ク図である。

図 8 9 は、メディアタイプ I M 1 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造工程の流れを示すフローチャートである。

図 9 0 は、メディアタイプ I M 2 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造装置の概略構成を示すブロック図である。

図 9 1 は、メディアタイプ I M 2 の光ディスク情報記録媒体に最新のリストを記録する光ディスク製造工程の流れを示すフローチャートである。

図 9 2 は、メディアタイプ I M 3 のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

図 9 3 は、メディアタイプ I M 3 のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

図 9 4 は、メディアタイプ I M 4 のメモリ情報記録媒体に最新のリストを記録するメモリ製造装置の概略構成を示すブロック図である。

図 9 5 は、メディアタイプ I M 4 のメモリ情報記録媒体に最新のリストを記録するメモリ製造工程の流れを示すフローチャートである。

図 9 6 は、媒体組立装置と情報書き込み装置からなる製造装置の概略構成を示すブロック図である。

## 発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

### 〔第 1 の実施の形態（IM2，Dev2）〕

図 1 には、本発明の第 1 の実施の形態に係る情報記録媒体の一例としての光ディスク情報記録媒体 10 の構成例を示す。

この光ディスク情報記録媒体 10 は、カートリッジ 11 内に、データを記録する光ディスク 12 と、不揮発性メモリ 34 を有するセキュリティモジュール 13 とを備えている。図 2 は、当該第 1 の実施の形態において不揮発性メモリ 34 を有するセキュリティモジュール 13 の構成例を示している。

セキュリティモジュール 13 は、図 2 に示すように、当該モジュール外の装置とデータの授受をするための接触式あるいは非接触式のインターフェース部 31 と、各種の演算を行うための演算部 32 と、乱数発生部 33 と、不揮発性メモリ 34 と、それらを制御するための制御部 35 とを備えている。

図 3 は、本発明の第 1 の実施の形態としての光ディスク記録再生装置 100 の構成例を示している。

この光ディスク記録再生装置 100 は、上記光ディスク情報記録媒体 10 を使用してデータの記録／再生を行うものであり、カートリッジ 11 内の光ディスク 12 を回転させるスピンドルモータ 101、光学ヘッド 102、サーボ回路 103、記録／再生回路 104、これらを制御する制御部 105、この制御部 105 に接続された入力部 106、乱数を発生する乱数発生部 107、不揮発性メモリ 1

10、インターフェース部108などを備えている。

スピンドルモータ101は、サーボ回路103によってその回転動作が制御され、光ディスク12を回転させる。光学ヘッド102は、レーザビームを光ディスク12の記録面に照射することで、データの記録／再生を行う。サーボ回路103は、スピンドルモータ101を駆動することにより、光ディスク12を所定の速度で（例えば線速度一定で）回転させる。また、サーボ回路103は、光学ヘッド102による光ディスク12へのトラッキング及びフォーカシングの他、上記光学ヘッド102をディスク半径方向に移動させる際のスレッドサーボ制御を行う。

そして、記録／再生回路104は、制御部105により動作モードが切り換えられる暗号化部104Aと復号部104Bを有する。暗号化部104Aは、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、光学ヘッド102に供給して、光ディスク12に記録させる。復号部104Bは、再生モード時に、光学ヘッド102により光ディスク12から再生されたデータを復号し、外部に再生信号として出力する。

また、入力部106は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部105は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部107は、制御部105の制御により、所定の乱数を発生する。インターフェース108部は、接触式あるいは非接触式であり、情報記録媒体10のセキュリティモジュール13との間でデータの授受を行う。

さらに、この第1の実施の形態の光ディスク記録再生装置100は、演算部109と不揮発性メモリ110を備えている。

ここで、本発明の第1の実施の形態において、上記光ディスク情報記録媒体10のセキュリティモジュール13は、個別の(1つの媒体毎)識別コード(ID)と、当該IDに対応する公開鍵暗号系のプライベート鍵(Private Key)とパブリック鍵(Public Key)、さらに信頼できるセンタ(Trusted Center:TC、以下、単にセンタTCと呼ぶ)からパブリック鍵証明書が与えられており、それら情報を不揮発性メモリ34或いは当該不揮発性メモリ34とは別の不揮発性の記憶領域に格納している。同じく、この第1の実施の形態の光ディスク記録再生装置100は、個別の(1台の装置毎の)識別コード(ID)と、当該IDに対応する公開鍵暗号系のプライベート鍵とパブリック鍵、センタTCからパブリック鍵証明書が与えられており、これら情報を不揮発性メモリ110或いは当該不揮発性メモリ110とは別の不揮発性の記憶領域に格納している。特に、プライベート鍵は外部に漏れないように、それぞれ不揮発性メモリ34、110或いはそれらとは別の記憶領域において安全に格納する。

上記光ディスク情報記録媒体10のセキュリティモジュール13に与えられている上記パブリック鍵証明書は、当該光ディスク情報記録媒体10のIDとパブリック鍵を含む情報に、センタTCがデジタル署名を施したデータである。同様に、光ディスク記録再生装置100に与えられているパブリック鍵証明書は、当該光ディスク記録再生装置100のIDとパブリック鍵を含む情報に、センタTCがデジタル署名を施したデータである。すなわち、これらパブリック鍵証明書は、個々の光ディスク情報記録媒体、及び、個々の光デ



ディスク記録再生装置が、それぞれ正当なものであることをセンタTCが認めることを証明する文書データであり、通常は、各記録媒体、装置がそれぞれ出荷される時に、センタTCから与えられるものである。なお、上記デジタル署名技術とは、あるデータを生成したのが、あるユーザであることを証明できる技術であり、例えばIEEE (Institute of Electrical and Electronics Engineers) P 1363で使用されているいわゆるECDSA (Elliptic Curve Digital Signature Algorithm) 方式などがよく知られている。

上記パブリック鍵証明書には、図4に示すように、エンティティID (Entity ID)、エンティティパブリック鍵 (Entity Public Key)、センタTCのデジタル署名の各項目が含まれる。なお、上記エンティティ (Entity) とは、本発明実施の形態の情報記録媒体または記録再生装置を指す。上記エンティティIDはそのエンティティに個別に与えられた識別番号である。また、各エンティティには、パブリック鍵とプライベート鍵のペアも個別に与えられ、そのうちパブリック鍵は上記パブリック鍵証明書に書かれ、プライベート鍵はそのエンティティが秘密に保持する。また、エンティティタイプ (Entity Type) とは、情報記録媒体又は記録再生装置が後述するリポケーションリスト (或いは後の第3の実施の形態で説明するレジストレーションリスト) 等を格納するための不揮発性メモリを備えたタイプであるか、或いは当該リストを格納するための不揮発性メモリを備えていないタイプであるか等、記録媒体の物理的構造を区別するための識別符号である。

また、この第1の実施の形態において、光ディスク情報記録媒体10の不揮発性メモリ34と光ディスク記録再生装置100の不揮

発性メモリ 110 には、それぞれ上記パブリック鍵証明書に含まれる上記センタ TC のデジタル署名を検証するために用いられる、システム全体で共通なセンタ TC のパブリック鍵がそれぞれ格納されている。

さらに、当該第 1 の実施の形態において、光ディスク情報記録媒体 10 のセキュリティモジュール 13 の不揮発性メモリ 34 と、光ディスク記録再生装置 100 の不揮発性メモリ 110 には、図 5 に示すリボケーションリストを格納する領域がそれぞれ設けられている。

上記リボケーションリストは、単調増加する番号であって当該リボケーションリストのバージョンを示すバージョンナンバーと、プライベート鍵が露呈してしまった光ディスク情報記録媒体或いは光ディスク記録再生装置の ID（リボークされる機器又は媒体の ID）のリストと、センタ TC によるデジタル署名とを有するものである。すなわち、リボケーションリストは、一般に不正者リスト或いはブラックリストとも呼ばれ、本実施の形態のような光ディスク情報記録媒体や光ディスク記録再生装置等から成るシステム全体においてその記録媒体又は装置のプライベート鍵が露呈してしまったもの（媒体又は装置）の ID がリストアップされ、それに対し信頼できるセンタ TC がデジタル署名を施したものである。したがって、あるエンティティ（情報記録媒体または記録再生装置）において、通信相手方の記録媒体若しくは装置の ID が当該リボケーションリストに載っていることを確認した場合、そのエンティティは通信相手方を不正なものと判断し、それ以上プロトコルを進めないようにすることができる。このことにより、プライベート鍵が露呈してし

まった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置を、このシステムから排除することが可能になる。また、光ディスク記録再生装置 100 を工場から出荷する際には、最新版のリボケーションリストを不揮発性メモリ 110 に格納して出荷する。

#### <第 1 の実施の形態の記録処理手順>

次に、図 6 から図 8 を用いて、第 1 の実施の形態の光ディスク記録再生装置 100 が光ディスク情報記録媒体 10 にデータを記録する手順を説明する。

なお、上述したように、第 1 の実施の形態の光ディスク記録再生装置 100 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 110 に格納しており、また同様に、当該第 1 の実施の形態の光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 34 に格納している。

まず、図 6 において、光ディスク記録再生装置 100 は、手順 R1 として、光ディスク情報記録媒体 10 のセキュリティモジュール 13 に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、1 回 1 回の記録を識別するために記録毎に割り当てられるレコーディング ID（Recording-ID）とを送る。

次に、手順 R2 として、光ディスク記録再生装置 100 及び光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、上記記

録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

ここで、公開鍵暗号技術を用いた相互認証プロトコルは、相手側が正しい（センタTCから承認を得た）パブリック鍵とプライベート鍵のペアを持っていることを互いに確認するプロトコルであり、例えばIEEE P1363で規格化作業中のECDSA (Elliptic Curve Digital Signature Algorithm) を用いることによって構成することができる。

なお、上記公開鍵暗号技術を用いた相互認証プロトコルにおいては、光ディスク情報記録媒体10のセキュリティモジュール13と光ディスク記録再生装置100の双方が、それぞれ乱数発生機能（セキュリティモジュール13の乱数発生部33、装置100の乱数発生部107）を用いて乱数を発生させること、不揮発性メモリに格納されている自己のプライベート鍵及びパブリック鍵証明書を読み出すこと、公開鍵暗号技術に基づく演算を演算機能（演算部）で行うこと、が必要となる。

また、公開鍵暗号技術を用いた相互認証プロトコルに対し、共通鍵暗号技術を用いた相互認証プロトコルも広く知られているが、当該相互認証プロトコルはその名の通り、プロトコルを実行する2者が共通の鍵を持っていることを前提とするプロトコルである。共通鍵暗号技術を用いた相互認証プロトコルを採用しようとした場合、記録媒体と記録再生装置のインターオペラビリティを確保する必要があるため、システム全体で共通の鍵をすべてのセキュリティモジュール13と光ディスク記録再生装置100が持つ必要がある。但し、この場合、一つのセキュリティモジュールあるいは光ディスク

記録再生装置が攻撃を受けて（解析されて）鍵が露呈してしまうと、その影響がシステム全体に広まってしまうという問題がある。

これに対し、公開鍵暗号技術を用いた相互認証プロトコルにおいては、各装置及び各セキュリティモジュールが持つ鍵は個別であり、しかも本実施の形態では上述したリボケーションリストを使用できるため、一つの装置或いは記録媒体の鍵が露呈したとしても、その装置或いは記録媒体だけをシステムから排除することができるので、影響を小さく抑えられるという利点がある。

上記公開鍵暗号技術を用いた鍵共有プロトコルは、2者間で安全に秘密情報を共有するためのプロトコルであり、やはり I E E E P 1 3 6 3 で規格化作業中のいわゆる E C - D H (Elliptic Curve Diffie Hellman) を用いることによって構成することができる。

公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実際に用いている例としては、I E E E 1 3 9 4 パス上のコンテンツプロテクション方式の一つである、ソニー、松下、日立、東芝、インテルの5社によって開発された、いわゆる D T C P (Digital Transmission Content Protection) 規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記した White Paper 或いは規格の Informational version を、ライセンス組織であるいわゆる D T L A (Digital Transmission Licensing Administrator) から誰でも取得することが可能である）の F A K E (Full Authentication and Key Exchange) プロトコルを挙げることができる。このプロトコルは、おおまかには下記のステップで構成される。

すなわち、当該プロトコルでは、先ず第1のステップとして、乱数発生器を用いて乱数を発生させ、不揮発性メモリから読み出した

自分のパブリック鍵証明書とともに他方に送る。

次に、当該プロトコルでは、第2のステップとして、相手のパブリック鍵証明書の正当性を公開鍵暗号技術に基づく演算を行って確かめる。

次に、当該プロトコルでは、第3のステップとして、鍵共有のための、公開鍵暗号技術に基づく演算（第1段階）を行い、公開鍵暗号技術に基づく演算を行って作成した自分のデジタル署名文とともに相手に送る。

その後、当該プロトコルでは、第4のステップとして、相手から送られた第3のステップでのデータについて、公開鍵暗号技術に基づく演算を行って相手のデジタル署名の検証を行い、鍵共有のための、公開鍵暗号技術に基づく演算（第2段階）を行って共有鍵の値を計算する。

本方式においては、上記相互認証を行う際に、相手の装置が正しいプライベート鍵とパブリック鍵のペアを持っていることのみならず、自分が持つリボケーションリストに相手の装置のIDが掲載されていないことを確認する。すなわち、出荷時には正当に鍵を持っていたが、それが例えばいわゆるリバースエンジニアリングなどの攻撃（不正な解析）を受け、鍵が露呈してしまった装置のIDが上記リボケーションリストに載せられているような場合には、当該リボケーションリストに載せられている装置（データを渡してはいけない装置）に対してデータを渡さずに済むようになる。

図6に戻り、さらに、上記手順R2では、記録再生装置と記録媒体のセキュリティモジュールとの間で、それぞれ自分が持っているリボケーションリストのバージョンナンバーを交換する。

次に、手順 R 3 , R 4 として、もし何れかの一方が他方のリボケーションリストより新しいリボケーションリストを持っていた場合、当該新しいリボケーションリストを持っている方は自分のリボケーションリストを他方に送る。一方、古いリボケーションリストを持っている方は、新しいリボケーションリストを持っている方から、当該新しいリボケーションリストを送ってもらい、その正当性を検証した後、自分が持つリボケーションリストを、その送られてきた新しいリボケーションリストに更新する。すなわち、手順 R 3 には、セキュリティモジュール上のリボケーションリストのバージョンが、記録再生装置上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順 R 4 には、記録再生装置上のリボケーションリストのバージョンが、セキュリティモジュール上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

なお、手順 R 3 , R 4 におけるリボケーションリストの送付は、後の手順 R 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 5 にてデータの記録を行った後に、手順 R 3 或いは R 4 でのリボケーションリストの送付を行うようにしてもよい。

さてここで、上述したような公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルの結果、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、安全に、ある値を共有することになる。以下、この共有される値をセッション鍵 (Session key : Kse) と呼ぶことにする。

次に、データを暗号化する暗号鍵 (Content key : Kco) を決定す

るが、その決定方法としては、例えば、以下に述べる暗号鍵決定方法（１）乃至暗号鍵決定方法（４）のうちの一つを用いればよい。

暗号鍵決定方法（１）：

$K_{co} = K_{se}$ とする。すなわち、上記の相互認証及び鍵共有プロトコルで得られたセッション鍵 $K_{se}$ を暗号鍵 $K_{co}$ とする。この時、セキュリティモジュール１３は、暗号鍵 $K_{co}$ を安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵（Storage key： $K_{st}$ ）を用いて当該暗号鍵 $K_{co}$ を暗号化した値 $E_{nc}(K_{st}, K_{co})$ を光ディスク記録再生装置１００に送り、光ディスク１２に記録させる。

暗号鍵決定方法（２）：

セキュリティモジュール１３が予め格納しているストレージ鍵 $K_{st}$ を暗号鍵 $K_{co}$ とする。この場合、セキュリティモジュール１３がストレージ鍵 $K_{st}$ を上記セッション鍵 $K_{se}$ で暗号化して光ディスク記録再生装置１００に送り、ストレージ鍵 $K_{st} (= k_{co})$ を用いてデータを暗号化して光ディスク１２に記録させる。

暗号鍵決定方法（３）：

セキュリティモジュール１３がそのデータ用の暗号鍵 $K_{co}$ を乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール１３が当該暗号鍵 $K_{co}$ を上記セッション鍵 $K_{se}$ で暗号化して光ディスク記録再生装置１００に送り、この装置１００において当該暗号鍵 $K_{co}$ を用いてデータを暗号化して光ディスク１２に記録させる。セキュリティモジュール１３は、暗号鍵 $K_{co}$ を安全にその内部の不揮発性メモリ３４に格納するか、セキュリティモジュール１３が予め格納しているストレージ鍵 $K_{st}$ を用いて上記暗号鍵 $K_{co}$



を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を光ディスク記録再生装置 100 に送り、光ディスク 12 に記録させる。

暗号鍵決定方法 (4) :

光ディスク記録再生装置 100 がそのデータ用の暗号鍵  $K_{co}$  を乱数発生器などを用いて新たに発生させ、当該暗号鍵  $K_{co}$  によりデータを暗号化して記録する。この場合、光ディスク記録再生装置 100 が暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化してセキュリティモジュール 13 に送る。セキュリティモジュール 13 は暗号鍵  $K_{co}$  を安全にその内部の不揮発性メモリ 34 に格納するか、セキュリティモジュール 13 が予め格納しているストレージ鍵  $K_{st}$  を用いて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を光ディスク記録再生装置 100 に送り、光ディスク 12 に記録させる。

上述した暗号鍵決定方法 (1) 乃至 (4) の何れかを用いて暗号鍵  $K_{co}$  を決定したならば、次に、手順 R5 として、光ディスク記録再生装置 100 は、光ディスク 12 に記録するデータを当該暗号鍵  $K_{co}$  で暗号化し、その暗号化されたデータ  $E_{nc}(K_{co}, data)$  を光ディスク 12 に記録する。

また、上記暗号鍵  $K_{co}$ 、又は暗号化した暗号鍵  $K_{co}$  を、セキュリティモジュール 13 の不揮発性メモリ 34 に記録する際には、レコーディング ID (Recording - ID) を検索用のキーとするために一緒に記録したり、データが記録される光ディスク 12 のセクタと同一のセクタに暗号化した  $K_{co}$  を記録するなどして、データと暗号鍵  $K_{co}$  の対応がとれるようにしておく。なお、この暗号鍵  $K_{co}$  の管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

共通鍵暗号アルゴリズムは、暗号化とその復号の処理に同一の暗号鍵を用いる暗号アルゴリズムであり、FIPS 46-2で米国の標準に指定されているいわゆるDES (Data Encryption Standard) をその例として挙げることできる。

特に、上記暗号鍵決定方法(4)の場合には、光ディスク記録再生装置100が暗号鍵 $K_{co}$ を決められるため、光ディスク記録再生装置100は予めデータを暗号化しておくことが可能になる。

当該第1の実施の形態では、以上の手順により、データを光ディスク12に記録する。

尚、上述の説明において、 $Enc(x, y)$ という表現は、 $x$ を鍵として $y$ を所定の暗号関数を用いて暗号化するという意味である。以降に関しても同様である。

#### <第1の実施の形態の記録処理手順(詳細1)>

次に、図7に、上記図6に示した第1の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10にデータを記録するまでの手順の詳細を示す。なお、この図7では、光ディスク記録再生装置100に係る各情報について「B」の文字を付し、光ディスク情報記録媒体10のセキュリティモジュール13に係る各情報について「A」の文字を付している。また、図6で説明したのと同様に、光ディスク記録再生装置100とセキュリティモジュール13は、センタTCから与えられたID(セキュリティモジュール13の $ID_A$ 、光ディスク記録再生装置100の $ID_B$ )、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ110, 34に格納している。

図7において、先ず、光ディスク記録再生装置100は、手順R11として、前記乱数発生部107にて64ビットの乱数 $R_B$ を生成し、この乱数 $R_B$ を記録コマンド（記録開始コマンド）と共にセキュリティモジュール13に送る。

上記記録コマンドと乱数 $R_B$ を受け取ったセキュリティモジュール13は、手順R12として、前記乱数発生部33にて64ビットの乱数 $R_A$ を発生すると共に、当該セキュリティモジュール13から外部に出力されることのない秘密の所定値或いは乱数の $K_A$  ( $0 < K_A < r$ ) を生成し、前記EC-DHアルゴリズムの第1段階（ステップ1）においてphase 1 value  $V_A$ の値を計算 ( $V_A = K_A \cdot G$ ) により求める。なお、 $V_A = K_A \cdot G$ は、いわゆる楕円関数を用いた暗号技術における楕円曲線上の演算であり、 $G$ は楕円曲線上のある点を表し、システムにおいて共通に設定されている値である。また、 $r$ は点 $G$ の位数である。更に、セキュリティモジュール13は、前記ECDSAの署名アルゴリズムを用いて、上記乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、リボケーションリストのバージョンナンバー $RevV_A$ からなるビット列 $R_A || R_B || V_A || RevV_A$ にデジタル署名の関数 $Sign$ を用いたデジタル署名を行い $Sig_A = Sign(PriKey_A, R_A || R_B || V_A || RevV_A)$ を得る。なお、 $PriKey_A$ はセキュリティモジュール13のプライベート鍵であり、「 $||$ 」はビットの連結を表している。セキュリティモジュール13は、これら $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $Sig_A$ にパブリック鍵証明書 $Cert_A$ を付け、光ディスク記録再生装置100に送る。なお、セキュリティモジュール13がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

上記セキュリティモジュール 13 から  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $Sig_A$ を受け取ると、光ディスク記録再生装置 100 は、E-CDSA の証明アルゴリズムを用いて、セキュリティモジュール 13 のパブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証（チェック）を行う。

すなわち、光ディスク記録再生装置 100 は、まず、セキュリティモジュール 13 のパブリック鍵証明書  $Cert_A$  の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 を不正な媒体とみなして当該プロトコルを終了する。

一方、セキュリティモジュール 13 のパブリック鍵証明書  $Cert_A$  の検証において正当であると判定された場合、光ディスク記録再生装置 100 は、上記パブリック鍵証明書  $Cert_A$  からパブリック鍵  $PubKey_A$  を手に入れる。次に、光ディスク記録再生装置 100 は、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と、当該光ディスク記録再生装置 100 が手順 R11 で生成した乱数  $R_B$  とが等しく、さらに上記デジタル署名  $Sig_A$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 が不正な媒体であると判断して当該プロトコルを終了する。

上述のように、セキュリティモジュール 13 から返送された乱数  $R_B$  が先に生成したものと等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、光ディスク記録再生装置 100 は、自己の不揮発性メモリ 110 に格納しているリボケーションリストを用い、セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10

の  $ID_A$  が当該リボケーションリストに掲載されていないことを検証する。この検証の結果、セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 の  $ID_A$  がリボケーションリストに掲載されている場合には、当該セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 は不正な媒体であると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 の  $ID_A$  が当該リボケーションリストに掲載されておらず、その光ディスク情報記録媒体 10 が正当であると判断した場合、光ディスク記録再生装置 100 は、手順 R13 として、当該装置 100 から外部に出力されることのない秘密の所定値或いは乱数の  $K_B$  ( $0 < K_B < r$ ) を生成し、前記 EC-DH アルゴリズムの第 1 段階 (ステップ 1) において  $pa$  値  $V_B$  を計算 ( $V_B = K_B \cdot G$ ) により求める。更に、光ディスク記録再生装置 100 は、前記 EC-DSA の署名アルゴリズムを用いて、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 100 が持つリボケーションリストのバージョンナンバー  $RevV_B$  からなるビット列  $R_B || R_A || V_B || RevV_B$  にデジタル署名の関数  $Sign$  を用いたデジタル署名を行い  $Sig_B = Sign(PriKey_B, R_B || R_A || V_B || RevV_B)$  を得る。なお、 $PriKey_B$  は光ディスク記録再生装置 100 のプライベート鍵である。光ディスク記録再生装置 100 は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 13 に送る。なお、光ディスク記録再生装置 100 がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記光ディスク記録再生装置 100 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 13 は、ECSA の証明アルゴリズムを用いて、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証（チェック）を行う。

すなわち、セキュリティモジュール 13 は、先ず、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$  の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置 100 を不正な装置とみなして当該プロトコルを終了する。

一方、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$  の検証において正当であると判定された場合、セキュリティモジュール 13 は、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 13 は、光ディスク記録再生装置 100 から返送されてきた乱数  $R_A$  と、当該セキュリティモジュール 13 が手順 R12 で生成した乱数  $R_A$  とが等しく、さらに上記デジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置 100 が不正な装置であると判断して当該プロトコルを終了する。

上述のように、光ディスク記録再生装置 100 から返送された乱数  $R_A$  と先に生成したものが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたとき、セキュリティモジュール 13 は、自己の不揮発性メモリ 34 に格納しているリボケーションリストを用い、光ディスク記録再生装置 100 の  $ID_B$  が当該リボケーションリストに掲載されていないことを検証する。この検証の結果、光ディスク記録再生装置 100 の  $ID_B$  がリボケーションリストに掲載されてい

る場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。

一方、光ディスク記録再生装置 100 の  $ID_B$  が当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわち、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 では  $K_A \cdot V_B$  の計算を行い、また、光ディスク記録再生装置 100 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュリティモジュール 13 と光ディスク記録再生装置 100 が共有する。

次に、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 R14 又は R15 として、その新しいバージョンのリボケーションリストを相手方に送る。すなわち、セキュリティモジュール 13 では、光ディスク記録再生装置 100 が保持しているリボケーションリストのバージョンナンバー  $RevV_B$  が、自己のリボケーションリストのバージョンナンバー  $RevV_A$  よりも新しいか否かチェックし、 $RevV_A$  が  $RevV_B$  よりも新しいとき、手順 R15 として、自己の保持しているリボケーションリストを光ディスク記録再生装置 100 に送る。一方、光ディスク記録再生装置 100 では、セキュリティモジュール 13 が保持しているリボケーションリストのバージョンナンバー  $RevV_A$  が、自己のリボケーションリストのバージョンナンバー  $RevV_B$  よりも新しいか否かチェックし、 $Re$

$vV_B$ が $RevV_A$ よりも新しいとき、手順R 1 4として、自己の保持しているリボケーションリストをセキュリティモジュール1 3に送る。

上述のように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタTCのデジタル署名TCSigを検証し、当該デジタル署名TCSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新（リストのアップデート）する。一方、デジタル署名TCSigが正しくない場合は、当該プロトコルを終了する。

その後、光ディスク記録再生装置1 0 0は、手順R 1 6として、光ディスク1 2に記録するコンテンツデータを暗号化するための暗号鍵（コンテンツ鍵）Kcoを定め、この暗号鍵Kcoをセッション鍵Kseにて暗号化した値 $E_{nc}(Kse, Kco)$ をセキュリティモジュール1 3に送信する。

セキュリティモジュール1 3は、手順R 1 7として、上記光ディスク記録再生装置1 0 0から送信されてきた値 $E_{nc}(Kse, Kco)$ をセッション鍵Kseを用いて復号することにより、暗号鍵Kcoを復元し、さらに、この暗号鍵Kcoを自己が持つストレージ鍵Kstにて暗号化した値 $E_{nc}(Kst, Kco)$ を光ディスク記録再生装置1 0-0に送信する。

セキュリティモジュール1 3から上記値 $E_{nc}(Kst, Kco)$ を受け取ると、光ディスク記録再生装置1 0 0は、手順R 1 8として、上記暗号鍵Kcoを用いて暗号化したコンテンツデータ $E_{nc}(Kco, data)$ を光ディスク情報記録媒体1 0の光ディスク1 2に記録すると共に、上記暗号鍵Kcoをストレージ鍵Kstにて暗号化した値 $E_{nc}(Ks$



t, Kco) も上記光ディスク情報記録媒体 10 の光ディスク 12 に記録する。

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### <第1の実施の形態の記録処理手順(詳細2)>

上記図7の例では、セキュリティモジュール13と光ディスク記録再生装置100において、手順R12, R13のように、自己が保持しているリボケーションリスト内にそれぞれ相手方のIDが掲載されているか否かの検証を行った後、手順R14, R15にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のIDがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

図8には、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示す。

この図8において、光ディスク記録再生装置100は、先ず、手

順 R 2 1 として、前記図 7 の手順 R 1 1 と同様に乱数  $R_B$  を生成し、この乱数  $R_B$  を記録コマンドと共にセキュリティモジュール 1 3 に送る。

上記記録コマンドと乱数  $R_B$  を受け取ったセキュリティモジュール 1 3 は、前記図 7 の手順 R 1 2 と同様に、手順 R 2 2 として、乱数  $R_A$  を発生すると共に前記所定値或いは乱数の  $K_A$  を生成し、 $V_A = K_A \cdot G$  の計算を行う。また、セキュリティモジュール 1 3 は、前記同様にビット列  $R_A || R_B || V_A || \text{Rev}V_A$  にデジタル署名を行い  $\text{Sig}_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$  を生成し、これら  $R_A$ ,  $R_B$ ,  $V_A$ ,  $\text{Rev}V_A$ ,  $\text{Sig}_A$  にパブリック鍵証明書  $\text{Cert}_A$  を付けて光ディスク記録再生装置 1 0 0 に送る。

上記セキュリティモジュール 1 3 から  $\text{Cert}_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $\text{Rev}V_A$ ,  $\text{Sig}_A$  を受け取ると、光ディスク記録再生装置 1 0 0 は、セキュリティモジュール 1 3 のパブリック鍵証明書  $\text{Cert}_A$ 、デジタル署名  $\text{Sig}_A$  の検証（チェック）を行う。

すなわち、光ディスク記録再生装置 1 0 0 は、先ず、セキュリティモジュール 1 3 のパブリック鍵証明書  $\text{Cert}_A$  の検証を行い、例えば当該検証をパスできないときには、そのセキュリティモジュール 1 3 を備えた光ディスク情報記録媒体 1 0 を不正な媒体とみなして当該プロトコルを終了する。

一方、セキュリティモジュール 1 3 のパブリック鍵証明書  $\text{Cert}_A$  の検証において正当であると判定された場合、光ディスク記録再生装置 1 0 0 は、上記パブリック鍵証明書  $\text{Cert}_A$  からパブリック鍵  $\text{PubKey}_A$  を手に入れる。次に、光ディスク記録再生装置 1 0 0 は、セキュリティモジュール 1 3 から返送されてきた乱数  $R_B$  と、当該光ディ

スク記録再生装置 100 が手順 R21 で生成した乱数  $R_B$  とが等しく、さらに上記デジタル署名  $Sig_A$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 が不正な媒体であると判断して当該プロトコルを終了する。

上述のように、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、光ディスク記録再生装置 100 は、図 7 の手順 R13 と同様に、手順 R23 として、 $K_B$  ( $0 < K_B < r$ ) を生成し、 $V_B = K_B \cdot G$  の計算を行う。更に、光ディスク記録再生装置 100 は、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、リボケーションリストバージョンナンバー  $RevV_B$  からなるビット列  $R_B || R_A || V_B || RevV_B$  にデジタル署名を行って  $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RevV_B)$  を生成し、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付けてセキュリティモジュール 13 に送る。

上記光ディスク記録再生装置 100 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 13 は、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。

すなわち、セキュリティモジュール 13 は、先ず、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$  の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置 100 を不正な装置とみなして当該プロトコルを終了する。

一方、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cer$

$t_B$ の検証において正当であると判定された場合、セキュリティモジュール 13 は、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 13 は、光ディスク記録再生装置 100 から返送されてきた乱数  $R_A$  と、当該セキュリティモジュール 13 が手順 R22 で生成した乱数  $R_A$  とが等しく、さらに上記デジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置 100 が不正な装置であると判断して当該プロトコルを終了する。

上述のように、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 では  $K_A \cdot V_B$  の計算を行い、また、光ディスク記録再生装置 100 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュリティモジュール 13 と光ディスク記録再生装置 100 が共有する。

また、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。すなわち、セキュリティモジュール 13 では、

光ディスク記録再生装置のID<sub>B</sub>が自己のリボケーションリストに掲載されていないことを検証し、光ディスク記録再生装置100では、セキュリティモジュール13のID<sub>A</sub>が自己のリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順R26の処理に進む。また、セキュリティモジュール13において、光ディスク記録再生装置100のID<sub>B</sub>が自己のリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置100は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置100において、セキュリティモジュール13のID<sub>A</sub>が自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール13は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール13と光ディスク記録再生装置100においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順R24又はR25として、上記新しいバージョンのリボケーションリストを相手方に送る。この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて、相手方のIDの検証を行う。すなわち、セキュリティモジュール13と光ディスク記録再生装置100は、それぞれが当該新しいバージョンのリボケーションリストを用いて、互いに相手方のIDの検証を行う。

すなわち例えば、セキュリティモジュール13のリボケーション

リストのバージョンが、光ディスク記録再生装置 100 のものよりも新しい場合、セキュリティモジュール 13 では自己が保持するリボケーションリストを用いて光ディスク記録再生装置 100 の ID<sub>B</sub> の検証を行い、その検証の結果、光ディスク記録再生装置 100 がリボケーションリストに記載されていないとき、手順 R24 として、自己が保持しているリボケーションリストを光ディスク記録再生装置 100 に送る。当該リボケーションリストを受け取った光ディスク記録再生装置 100 は、この送られてきたリボケーションリストのバージョンナンバー RevV<sub>A</sub> を先に取得しているバージョンナンバーと同じかどうかチェックし、さらに、その新しいリボケーションリストを用いてセキュリティモジュール 13 の ID<sub>A</sub> の検証を行う。その検証の結果、セキュリティモジュール 13 の ID<sub>A</sub> がリボケーションリストに記載されていない場合には、上記セキュリティモジュール 13 から送られてきた当該新しいバージョンのリボケーションリスト内に含まれるセンタ TC のデジタル署名 TC Sig を検証し、このデジタル署名 TC Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、デジタル署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

また例えば、光ディスク記録再生装置 100 のリボケーションリストのバージョンが、セキュリティモジュール 13 のものよりも新しい場合、光ディスク記録再生装置 100 では自己が保持するリボケーションリストを用いてセキュリティモジュール 13 の ID<sub>A</sub> の検証を行い、その検証の結果、セキュリティモジュール 13 がリボケーションリストに記載されていないとき、手順 R25 として、自己

が保持しているリボケーションリストをセキュリティモジュール 13 に送る。当該リボケーションリストを受け取ったセキュリティモジュール 13 は、この送られてきたリボケーションリストのバージョンナンバー  $RevV_B$  を先に取得しているバージョンナンバーと同一かどうかチェックし、さらに、その新しいリボケーションリストを用いて光ディスク記録再生装置 100 の  $ID_B$  の検証を行い、その検証の結果、光ディスク記録再生装置 100 の  $ID_B$  がリボケーションリストに記載されていないとき、上記光ディスク記録再生装置 100 から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタ  $TC$  のデジタル署名  $TC\text{Sig}$  を検証し、当該デジタル署名  $TC\text{Sig}$  が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、デジタル署名  $TC\text{Sig}$  が正しくない場合は、当該プロトコルを終了する。

その後、光ディスク記録再生装置 100 は、手順 R 26 として、光ディスク 12 に記録するコンテンツデータを暗号化するための暗号鍵  $K_{co}$  を定め、この暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  にて暗号化した値  $E_{nc}(K_{se}, K_{co})$  をセキュリティモジュール 13 に送信する。

セキュリティモジュール 13 は、手順 R 27 として、上記光ディスク記録再生装置 100 から送信されてきた値  $E_{nc}(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することにより、暗号鍵  $K_{co}$  を復元し、さらに、この暗号鍵  $K_{co}$  を自己が持つストレージ鍵  $K_{st}$  にて暗号化した値  $E_{nc}(K_{st}, K_{co})$  を光ディスク記録再生装置 100 に送信する。

セキュリティモジュール 13 から上記値  $E_{nc}(K_{st}, K_{co})$  を受け取ると、光ディスク記録再生装置 100 は、手順 R 28 として、上

記暗号鍵  $K_{co}$  を用いて暗号化したコンテンツデータ  $E_{nc}(K_{co}, data)$  を光ディスク情報記録媒体 10 の光ディスク 12 に記録すると共に、上記暗号鍵  $K_{co}$  をストレージ鍵  $K_{st}$  にて暗号化した値  $E_{nc}(K_{st}, K_{co})$  も上記光ディスク情報記録媒体 10 の光ディスク 12 に記録する。

#### < 第 1 の実施の形態の再生処理手順 >

次に、図 9 乃至図 11 を用いて、上記第 1 の実施の形態の光ディスク記録再生装置 100 が光ディスク 12 からデータを再生する手順を説明する。

なお、上述したように、第 1 の実施の形態の光ディスク記録再生装置 100 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 110 に格納しており、また同様に、当該第 1 の実施の形態の光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 34 に格納している。また、光ディスク記録再生装置 100 は、再生すべきデータに付与されたレコーディング ID (Recording-ID) を知っているものとする。

先ず、図 9 において、光ディスク記録再生装置 100 は、手順 P1 として、光ディスク情報記録媒体 10 のセキュリティモジュール 13 に対して、これからデータの再生を行うことを示す再生コマンド (再生開始コマンド) とレコーディング ID とを送る。

次に、手順 P2 として、光ディスク記録再生装置 100 及び光デ



ィスク情報記録媒体 10 のセキュリティモジュール 13 は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。

このプロトコルの内容は、データの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つパブリック鍵とプライベート鍵が正しいことの検証と、リボケーションリストに相手方の ID が載せられていないことの確認を互に行い、セッション鍵  $K_{se}$  を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。また、手順 P 3, P 4 として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。

次に、データを光ディスク 12 から読み出す前に、このデータを暗号化したときの暗号鍵  $K_{co}$  を光ディスク記録再生装置 100 が知ることが必要になる。

暗号鍵  $K_{co}$  は、セキュリティモジュール 13 が安全にその内部の不揮発性メモリ 34 に格納しているか、或いはセキュリティモジュール 13 が予め格納しているストレージ鍵  $K_{st}$  を用いて当該暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  として光ディスク 12 に記録されている。

前者の場合、セキュリティモジュール 13 は、手順 P 5 として、不揮発性メモリ 34 に格納されている暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化した値  $E_{nc}(K_{se}, K_{co})$  を、光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 では、当該値  $E_{nc}(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することにより暗号鍵  $K$

coを得る。

一方、後者の場合、光ディスク記録再生装置 100 は、先ず、光ディスク 12 から上記暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を読み出し、これをセキュリティモジュール 13 に送る。セキュリティモジュール 13 は、ストレージ鍵  $K_{st}$  を用いてこれを復号して暗号鍵  $K_{co}$  を得、これをセッション鍵  $K_{se}$  で暗号化した値  $E_{nc}(K_{se}, K_{co})$  を、手順 P5 として光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 は、当該値  $E_{nc}(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することにより暗号鍵  $K_{co}$  を得る。

上述のように、光ディスク記録再生装置 100 は、手順 P5 により、データを暗号化したときの暗号鍵  $K_{co}$  を得ることができる。

次に、手順 P6 として、光ディスク記録再生装置 100 は、光ディスク 12 から、上記暗号鍵  $K_{co}$  を用いて暗号化されているデータ  $E_{nc}(K_{co}, data)$  を読み出し、先に取得した暗号鍵  $K_{co}$  を用いてこれを復号し使用する。

以上が、光ディスク 12 からデータを読み出す処理の基本的な手順である。

#### < 第 1 の実施の形態の再生処理手順 (詳細 1) >

図 10 には、上記図 7 に示した第 1 の実施の形態の光ディスク記録再生装置 100 が、光ディスク情報記録媒体 10 の光ディスク 12 から、上記暗号化されているデータを読み出すまでの手順の詳細を説明する。なお、この図 10 では、前述の図 7 等と同様に、光ディスク記録再生装置 100 に係る各情報について「B」の文字を付し、セキュリティモジュール 13 に係る各情報について「A」の文字を付している。また、図 9 で説明したのと同様に、光ディスク記

録再生装置 100 とセキュリティモジュール 13 は、センタ TC から与えられた ID (セキュリティモジュール 13 の  $ID_A$ 、光ディスク記録再生装置 100 の  $ID_B$ )、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ 110, 34 に格納している。

図 10 において、先ず、光ディスク記録再生装置 100 は、手順 P11 として、前記記録時と同様に、乱数発生部 107 にて 64 ビットの乱数  $R_B$  を生成し、この乱数  $R_B$  を再生コマンド (再生開始コマンド) と共にセキュリティモジュール 13 に送る。

上記再生コマンドと乱数  $R_B$  を受け取ったセキュリティモジュール 13 は、手順 P12 として、前記記録時と同様に、乱数発生部 33 にて 64 ビットの乱数  $R_A$  を発生すると共に、前記同様の秘密の所定値或いは乱数の  $K_A$  ( $0 < K_A < r$ ) を生成し、前記 EC-DH アルゴリズムの第 1 段階 (ステップ 1) において  $V_A = K_A \cdot G$  の計算を行い、更に、前記 EC-DSA の署名アルゴリズムを用いて、上記乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、リボケーションリストのバージョンナンバー  $RevV_A$  からなるビット列  $R_A || R_B || V_A || RevV_A$  にデジタル署名を行った  $Sig_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || RevV_A)$  を得る。セキュリティモジュール 13 は、これら  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $Sig_A$  にパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 100 に送る。

上記セキュリティモジュール 13 から  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $Sig_A$  を受け取ると、光ディスク記録再生装置 100 は、前述の記録時と同様に、EC-DSA の証明アルゴリズムを用いて、セキュリティモジュール 13 のパブリック鍵証明書  $Cert_A$ 、デジタ

ル署名  $Sig_A$ 、 $ID_A$  の検証（チェック）を行う。すなわち、光ディスク記録再生装置 100 は、セキュリティモジュール 13 のパブリック鍵証明書  $Cert_A$  の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合には、上記パブリック鍵証明書  $Cert_A$  からパブリック鍵  $PubKey_A$  を手に入れる。

次に、光ディスク記録再生装置 100 は、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と上記手順 P 11 で生成した乱数  $R_B$  とが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 が不正な媒体であると判断して当該プロトコルを終了する。

上記セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、前述の記録時と同様に、光ディスク記録再生装置 100 は、自己が保持しているリボケーションリストを用い、セキュリティモジュール 13 の  $ID_A$  が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記  $ID_A$  がリボケーションリストに掲載されている場合には、当該セキュリティモジュール 13 を備えた光ディスク情報記録媒体 10 は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記  $ID_A$  が当該リボケーションリストに掲載されておらず正当な媒体であると判断した場合、光ディスク記録再生装置 100 は、手順 P 13 として、前記録時と同様に、所定値或いは乱数の  $K_B$  ( $0 < K_B < r$ ) を生成し、

前記 E C - D H アルゴリズムの第 1 段階 (ステップ 1) において  $V_B = K_B \cdot G$  の計算を行い、更に、前記 E C - D S A の署名アルゴリズムを用いて、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、バージョンナンバー  $RevV_B$  からなるビット列  $R_B || R_A || V_B || RevV_B$  にデジタル署名を行って  $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RevV_B)$  を得る。光ディスク記録再生装置 100 は、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 13 に送る。

上記光ディスク記録再生装置 100 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 13 は、E C - D S A の証明アルゴリズムを用いて、光ディスク記録再生装置 100 のパブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証 (チェック) を行う。すなわち、セキュリティモジュール 13 は、先ずパブリック鍵証明書  $Cert_B$  の検証を行い、例えば当該検証をパスできないときには、その光ディスク記録再生装置 100 を不正な装置とみなして当該プロトコルを終了し、一方、上記パブリック鍵証明書  $Cert_B$  の検証において正当であると判定された場合、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 13 は、光ディスク記録再生装置 100 から返送されてきた乱数  $R_A$  と、先に手順 P 12 で生成した乱数  $R_A$  とが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合には光ディスク記録再生装置 100 が不正な装置であると判断して当該プロトコルを終了する。

上述のように、光ディスク記録再生装置 100 から返送されてき

た乱数  $R_A$  と先に生成したものが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたとき、セキュリティモジュール 13 は、自己が保持するリボケーションリストに光ディスク記録再生装置 100 の  $ID_B$  が記載されていないことを検証し、その検証の結果、光ディスク記録再生装置 100 の  $ID_B$  がリボケーションリストに掲載されている場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。

光ディスク記録再生装置 100 の  $ID_B$  が当該リボケーションリストに掲載されておらず、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわちセキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 では  $K_A \cdot V_B$  の計算を行い、また、光ディスク記録再生装置 100 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュリティモジュール 13 と光ディスク記録再生装置 100 が共有する。

次に、前記記録時と同様に、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 P14 又は P15 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタ  $TC$  のデジタル署名  $TC\text{Sig}$  を検証し、当該デジタル署名  $TC\text{Sig}$  が正しい場合にのみ、そのリボケーションリストを用い

て自己が保持している古いリボケーションリストを更新（リストのアップデート）する。

次に、光ディスク記録再生装置 100 は、暗号化されているデータを光ディスク 12 から読み出す前に、このデータを暗号化したときの暗号鍵  $K_{co}$  を取得し、当該取得した暗号鍵  $K_{co}$  を用いて、上記光ディスク 12 から読み出した暗号化されているデータを復号する。なお、図 10 の例では、セキュリティモジュール 13 がストレージ鍵  $K_{st}$  を用いて暗号化した値  $E_{nc}(K_{st}, K_{co})$  が光ディスク 12 に記録されているとする。この場合、光ディスク記録再生装置 100 は、先ず、手順 P 16 として、光ディスク 12 から上記ストレージ鍵  $K_{st}$  で暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を読み出し、次に手順 P 17 として、当該値  $E_{nc}(K_{st}, K_{co})$  をセキュリティモジュール 13 に送る。セキュリティモジュール 13 では、予め保持しているストレージ鍵  $K_{st}$  を用いてこれを復号して暗号鍵  $K_{co}$  を得、当該暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化し、その値  $E_{nc}(K_{se}, K_{co})$  を手順 P 18 として光ディスク記録再生装置 100 に送る。光ディスク記録再生装置 100 は、当該値  $E_{nc}(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することで、暗号鍵  $K_{co}$  を得る。

その後、光ディスク記録再生装置 100 は、手順 P 19 により、暗号鍵  $K_{co}$  にて暗号化されているデータ  $E_{nc}(K_{co}, \text{data})$  を光ディスク 12 から読み出し、これを先に取得した暗号鍵  $K_{co}$  を用いて復号する。

#### < 第 1 の実施の形態の再生処理手順（詳細 2） >

上記図 10 の例では、セキュリティモジュール 13 と光ディスク記録再生装置 100 において、手順 P 12, P 13 のように、自己

が保持しているリボケーションリスト内にそれぞれ相手方のIDが掲載されているか否かの検証を行った後、手順P14, P15にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、当該再生の場合も前述した記録の場合と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のIDがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、この再生の例の場合も、前述の図8の例と同様に、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

図11には、光ディスク12からのデータ再生時において、上述したように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDを検証するようにした場合の手順を示す。

この図11において、光ディスク記録再生装置100は、まず、手順P21として、前記図10の手順P11と同様に乱数 $R_B$ を生成し、この乱数 $R_B$ を再生コマンドと共にセキュリティモジュール13に送る。

上記再生コマンドと乱数 $R_B$ を受け取ったセキュリティモジュール13は、前記図10の手順P12と同様に、手順P22として、乱数 $R_A$ と前記所定値或いは乱数の $K_A$ を生成し、 $V_A = K_A \cdot G$ の計算



を行い、更に前記同様にビット列  $R_A || R_B || V_A || \text{Rev}V_A$  にデジタル署名を行って  $\text{Sig}_A = \text{Sign}(\text{PriKey}_A, R_A || R_B || V_A || \text{Rev}V_A)$  を生成し、これらにパブリック鍵証明書  $\text{Cert}_A$  を付けて光ディスク記録再生装置 100 に送る。

上記セキュリティモジュール 13 から  $\text{Cert}_A, R_A, R_B, V_A, \text{Rev}V_A, \text{Sig}_A$  を受け取ると、光ディスク記録再生装置 100 は、セキュリティモジュール 13 のパブリック鍵証明書  $\text{Cert}_A$  とデジタル署名  $\text{Sig}_A$  の検証を行う。すなわち、光ディスク記録再生装置 100 は、上記パブリック鍵証明書  $\text{Cert}_A$  の検証を行い、当該パブリック鍵証明書  $\text{Cert}_A$  の検証において正当であると判定された場合に、上記パブリック鍵証明書  $\text{Cert}_A$  からパブリック鍵  $\text{PubKey}_A$  を手に入れ、次に、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と手順 P 21 で生成した乱数  $R_B$  とが等しく、且つデジタル署名  $\text{Sig}_A$  が正当であると判定されたときのみ次の処理に進む。

上述のように正当であると判定されたとき、光ディスク記録再生装置 100 は、図 10 の手順 P 13 と同様に、手順 P 23 として、 $K_B$  ( $0 < K_B < r$ ) を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、バージョンナンバー  $\text{Rev}V_B$  からなるビット列  $R_B || R_A || V_B || \text{Rev}V_B$  にデジタル署名を行って  $\text{Sig}_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || \text{Rev}V_B)$  を生成し、これら  $R_B, R_A, V_B, \text{Rev}V_B, \text{Sig}_B$  にパブリック鍵証明書  $\text{Cert}_B$  を付けてセキュリティモジュール 13 に送る。

上記光ディスク記録再生装置 100 から  $\text{Cert}_B, R_B, R_A, V_B, \text{Rev}V_B, \text{Sig}_B$  を受け取ると、セキュリティモジュール 13 は、光ディスク記録再生装置 100 のパブリック鍵証明書  $\text{Cert}_B$ 、デジタ

ル署名  $Sig_B$  の検証を行う。セキュリティモジュール 13 は、上記パブリック鍵証明書  $Cert_B$  の検証の結果、正当であると判定された場合、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れ、次に、光ディスク記録再生装置 100 から返送されてきた乱数  $R_A$  と前記手順 P 22 で生成した乱数  $R_A$  とが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたとき、次の処理に進む。

上述のように、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 では  $K_A \cdot V_B$  の計算を行い、光ディスク記録再生装置 100 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュリティモジュール 13 と光ディスク記録再生装置 100 が共有する。また、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。

一方、セキュリティモジュール 13 と光ディスク記録再生装置 100 においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持し

ているバージョンよりも他方のバージョンが新しい場合、手順 P 2 4 又は P 2 5 として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いた相手方の ID 検証を行うと共に、古いバージョンのリボケーションリストを更新する。

その後、光ディスク記録再生装置 1 0 0 は、手順 P 2 6 として、光ディスク 1 2 から上記ストレージ鍵  $K_{st}$  で暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を読み出し、次に手順 P 2 7 として、当該値  $E_{nc}(K_{st}, K_{co})$  をセキュリティモジュール 1 3 に送る。セキュリティモジュール 1 3 において、ストレージ鍵  $K_{st}$  により復号され、更にセッション鍵  $K_{se}$  で暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{se}, K_{co})$  は、手順 P 2 8 として光ディスク記録再生装置 1 0 0 に送られ、光ディスク記録再生装置 1 0 0 では、当該値  $E_{nc}(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することで、暗号鍵  $K_{co}$  を得る。その後、光ディスク記録再生装置 1 0 0 は、手順 P 2 9 により、光ディスクから、データ  $E_{nc}(K_{co}, data)$  を読み出し、先に取得した暗号鍵  $K_{co}$  を用いて、その復号を行う。

#### 〔第 2 の実施の形態 (IM4, Dev4)〕

次に、本発明の第 2 の実施の形態について説明する。

本発明の第 2 の実施の形態では、情報記録媒体として、メモリ情報記録媒体を用いる。

図 1 2 には、本実施の形態のメモリ情報記録媒体 2 0 の構成例を示す。

このメモリ情報記録媒体 2 0 は、カートリッジ 2 1 内に、データ

を記録するための電氣的に消去可能な大容量不揮発性メモリ（具体的には例えばフラッシュROMやEEPROM、磁気抵抗効果を用いたMRAM（Magnetic Random Access Memory）など）からなるメモリ部22と、セキュリティモジュール23及び入出力端子24を備えている。

上記セキュリティモジュール23は、図13に示すように、主要構成要素として、外部インターフェース部41、演算部42、乱数発生部43、不揮発性メモリ44、制御部45、記録媒体インターフェース部46を備えている。

すなわち、このセキュリティモジュール23は、図2に示したセキュリティモジュール13と略々同じ構成及び機能を有するが、当該セキュリティモジュール23の場合、外部とのインターフェース手段として外部インターフェース部41を備えている。また、このセキュリティモジュール23は、カートリッジ21内のメモリ部22との間のインターフェースをとるための記録媒体インターフェース（例えばフラッシュROMインターフェースなど）46を備えており、したがって、前記メモリ部22への情報の記録（書き込み）、再生（読み出し）は、当該セキュリティモジュール23を介して行われる。

このセキュリティモジュール23内部の不揮発性メモリ44は、秘密性の必要な情報や耐改ざん性が必要な情報など、重要な情報を格納するのに用いられるが、もしこのメモリ44の容量が十分でない場合には、セキュリティモジュール23外の、一般データを記録するための大容量のメモリ部22にこれらの重要な情報を記録することもできる。この場合、秘密性の必要な情報については、セキ

リティモジュール 23 内の不揮発性メモリ 44 に安全に格納してあるストレージ鍵  $K_{st}$  により暗号化するなどの方法を用いて保護し、耐改ざん性の必要な情報については、重要な情報を記録するメモリ部 22 のブロックのいわゆる ICV (Integrity Check Value) を計算し、セキュリティモジュール 23 内の不揮発性メモリ 44 に格納しておき、セキュリティモジュール 23 外のメモリ部 22 から情報を読み出す際に再びそのブロックの ICV を計算し、格納してある値と比較することによって情報が改ざんされていないことを確認するなどの保護策をとる。

ICV は、あるデータの完全性 (Integrity、改ざんされていないこと) を保証するために、データと、何らかの秘密値 (この場合、例えばセキュリティモジュール 23 のストレージ鍵  $K_{st}$ ) とを入力とし、予め定められたアルゴリズムによって計算される値である。これによれば、上記の秘密値を知っているものしか任意のデータに対する ICV を計算することが事実上できないため、例えばデータが変更されたような場合には、読み出し時に同様の方法で計算される ICV と記録時に計算されてセキュリティモジュール 23 内に格納されている値とが異なることになり、上記データが変更された事実をセキュリティモジュール 23 は知ることができるようになる。

なお、ICV を計算するアルゴリズムとしては、公開鍵暗号技術を用いたデジタル署名アルゴリズムや、共通鍵暗号技術を用いた MAC (Message Authentication Code) 作成アルゴリズム、鍵つきハッシュ関数を用いるアルゴリズムなどがある。ICV については、例えば、Menezes 等の、「Handbook of applied cryptography」、CRC、ISBN 0-8493-8523-7、pp. 352 - 368 に詳しい解説がある。

図 1 4 は、上記第 2 の実施の形態のメモリ情報記録媒体 2 0 に対してデータ等の記録／再生（書き込み／読み出し）を行うメモリ記録再生装置 2 0 0 の構成例を表している。

この図 1 4 に示したメモリ記録再生装置 2 0 0 は、主要構成要素として、入出力端子 2 0 1、制御部 2 0 5、入力部 2 0 6、乱数発生部 2 0 7、インターフェース部 2 0 8、演算部 2 0 9、不揮発性メモリ 2 1 0などを備えて成る。

このメモリ記録再生装置 2 0 0 は、図 3 に示した光ディスク記録再生装置 1 0 0 とその構成が略々同じであるが、図 3 における光ディスク 1 2 用の構成要素であるスピンドルモータ 1 0 1、光学ヘッド 1 0 2 やサーボ回路 1 0 3 などは存在せず、その代わりに、セキュリティモジュール 2 3 を介してメモリ情報記録媒体 2 0 への記録／再生のためのインターフェースが設けられる。なお、図 1 4 の例では、セキュリティモジュール 2 3 にアクセスするためのインターフェース部 2 0 8 が、上記メモリ情報記録媒体 2 0 への記録／再生のためのインターフェースの機能を兼用している。また、この図 1 4 の場合、メモリ情報記録媒体 2 0 の入出力端子 2 4 と、メモリ記録再生装置 2 0 0 の入出力端子 2 0 1 が電氣的に接続される。

記録／再生回路 2 0 4 は、制御部 2 0 5 により動作モードが切り換えられる暗号化部 2 0 4 A と復号部 2 0 4 B を有する。暗号化部 2 0 4 A は、記録モード時に、外部から記録信号の供給を受けると、その記録信号を暗号化し、インターフェース部 2 0 8 に供給して、メモリ情報記録媒体 2 0 のメモリ部 2 2 に記録させる。復号部 2 0 4 B は、再生モード時に、メモリ情報記録媒体 2 0 のメモリ部 2 2 から再生されたデータを復号し、外部に再生信号として出力する。

また、入力部 206 は、前記図 3 の入力部 106 と同様に、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作がなされたとき、その入力操作に対応する信号を出力する。制御部 205 は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部 207 は、制御部 205 の制御により、所定の乱数を発生する。インターフェース 208 部は、メモリ情報記録媒体 20 の入出力端子 24 及びメモリ記録再生装置 200 の入出力端子 201 を介して、メモリ情報記録媒体 20 のセキュリティモジュール 23 との間でデータの授受を行う。

さらに、この第 2 の実施の形態のメモリ記録再生装置 200 は、演算部 209 と不揮発性メモリ 210 をも備えている。これら演算部 209 及び不揮発性メモリ 210 は、前記図 3 の構成の演算部 109 及び不揮発性メモリ 110 と同様の機能を有している。

#### <第 2 の実施の形態の記録処理手順>

次に、図 15 から図 18 を用いて、第 2 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 20 にデータを記録する手順を説明する。

なお、当該第 2 の実施の形態のメモリ記録再生装置 200 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 210 に格納しており、また同様に、当該第 2 の実施の形態のメモリ情報記録媒体 20 のセキュリティモジュール 23 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリ

ストを上記不揮発性メモリ 44 に格納している。

先ず、図 15 において、メモリ記録再生装置 200 は、手順 R 31 として、メモリ情報記録媒体 20 のセキュリティモジュール 23 に対して、これからデータの記録を行うことを示す記録コマンド（記録開始コマンド）と、1 回 1 回の記録を識別するために記録毎に割り当てられるレコーディング ID (Recording-ID) とを送る。

次に、手順 R 32 として、メモリ記録再生装置 200 及びメモリ情報記録媒体 20 のセキュリティモジュール 23 は、上記記録コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第 1 の実施の形態におけるデータの記録時に用いられるプロトコルと同様であり、それぞれ他方が持つパブリック鍵とプライベート鍵が正しいことの検証と、リボケーションリストに相手方の ID が載せられていないことの確認を互いに行い、セッション鍵 K<sub>se</sub> を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

また、前記図 6 の手順 R 3, R 4 と同様に、図 15 の手順 P 33, P 34 として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順 R 33 には、セキュリティモジュール 23 上のリボケーションリストのバージョンが、記録再生装置 200 上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順 R 34 には、記録再生装置 200 上のリボケーションリストのバージョンが、セキュリティモ



ジュール 2 3 上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

なお、手順 R 3 3, R 3 4 におけるリボケーションリストの送付は、後の手順 R 3 5, R 3 6 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 3 5, R 3 6 にてデータの記録を行った後に、手順 R 3 3 或いは R 3 4 でのリボケーションリストの送付を行うようにしてもよい。

ここで、当該第 2 の実施の形態においても前記第 1 の実施の形態の場合と同様に、データを暗号化する暗号鍵  $K_{co}$  を決定するが、その決定方法としては、以下に述べる暗号鍵決定方法 (1 1) 乃至暗号鍵決定方法 (1 4) のうちの一つを用いればよい。

暗号鍵決定方法 (1 1) :

$K_{co} = K_{se}$  とする。すなわち、上記の相互認証及び鍵共有プロトコルで得られたセッション鍵  $K_{se}$  を暗号鍵  $K_{co}$  とする。この時、セキュリティモジュール 2 3 は、暗号鍵  $K_{co}$  を安全にその内部の不揮発性メモリ 4 4 に格納するか、セキュリティモジュール 2 3 が予め格納しているストレージ鍵  $K_{st}$  を用いて当該暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を、当該セキュリティモジュール 2 3 外のメモリ部 2 2 に格納する。

暗号鍵決定方法 (1 2) :

セキュリティモジュール 2 3 が予め格納しているストレージ鍵  $K_{st}$  を暗号鍵  $K_{co}$  とする。この場合、セキュリティモジュール 2 3 がストレージ鍵  $K_{st}$  を上記セッション鍵  $K_{se}$  で暗号化してメモリ記録再生装置 2 0 0 に送る。

暗号鍵決定方法 (1 3) :

セキュリティモジュール 23 がそのデータ用の暗号鍵  $K_{co}$  を乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール 23 が当該暗号鍵  $K_{co}$  を上記セッション鍵  $K_{se}$  で暗号化してメモリ記録再生装置 200 に送る。また、セキュリティモジュール 23 は、暗号鍵  $K_{co}$  を安全にその内部の不揮発性メモリ 44 に格納するか、セキュリティモジュール 23 が予め格納しているストレージ鍵  $K_{st}$  を用いて上記暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を上記メモリ部 22 に格納する。

暗号鍵決定方法 (14) :

メモリ記録再生装置 200 がそのデータ用の暗号鍵  $K_{co}$  を乱数発生器などを用いて新たに発生させる。この場合、メモリ記録再生装置 200 が暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化してセキュリティモジュール 23 に送る。セキュリティモジュール 23 は暗号鍵  $K_{co}$  を安全にその内部の不揮発性メモリ 44 に格納するか、セキュリティモジュール 23 が予め格納しているストレージ鍵  $K_{st}$  を用いて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  を上記メモリ部 22 に格納する。

上述した暗号鍵決定方法 (11) 乃至 (14) の何れかを用いて暗号鍵  $K_{co}$  を決定したならば、次に、手順 R35 として、メモリ記録再生装置 200 は、メモリ情報記録媒体 20 のメモリ部 22 に記録するデータを当該暗号鍵  $K_{co}$  で暗号化し、その暗号化されたデータ  $E_{nc}(K_{co}, data)$  をセキュリティモジュール 23 に伝送する。

この時のセキュリティモジュール 23 は、手順 R36 として、当該暗号化されたデータ  $E_{nc}(K_{co}, data)$  を、上記大容量のメモリ部 22 に格納する。

また、上記暗号鍵  $K_{co}$ 、又は暗号化した暗号鍵  $K_{co}$  を、セキュリティモジュール 23 の不揮発性メモリ 44、又はメモリ部 22 に記録する際には、レコーディング ID を検索用のキーとするために一緒に記録したり、データが記録されるメモリ部 22 のセクタと同一のセクタに、上記暗号化した暗号鍵  $K_{co}$  を記録するなどして、データと暗号鍵  $K_{co}$  との対応がとれるようにしておく。なお、この暗号鍵  $K_{co}$  の管理、伝送と、データの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが好適である。

また特に、上記暗号鍵決定方法 (14) の場合には、メモリ記録再生装置 200 が暗号鍵  $K_{co}$  を決められるため、メモリ記録再生装置 200 は予めデータを暗号化しておくことが可能になる。

当該第 2 の実施の形態では、以上の手順により、データをメモリ情報記録媒体 20 の大容量メモリ部 22 に記録する。

#### < 第 2 の実施の形態の記録処理手順 (詳細 1) >

次に、図 16 には、上記図 15 に示した第 2 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 20 にデータを記録するまでの手順の詳細を示す。なお、この図 16 では、メモリ記録再生装置 200 に係る各情報について「B」の文字を付し、メモリ情報記録媒体 20 のセキュリティモジュール 23 に係る各情報について「A」の文字を付している。また、図 15 で説明したのと同様に、メモリ記録再生装置 200 とセキュリティモジュール 23 は、センタ TC から与えられた ID (セキュリティモジュール 23 の ID<sub>A</sub>、メモリ記録再生装置 200 の ID<sub>B</sub>)、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ 210, 44 に格納してい

る。

図16の手順R41乃至手順R46までは、前述した第1の実施の形態における図7の手順R11乃至手順R16までと略々同じである。

すなわち、メモリ記録再生装置200は、手順R41として乱数 $R_B$ を生成して記録コマンドと共にセキュリティモジュール23に送り、当該記録コマンドと乱数 $R_B$ を受け取ったセキュリティモジュール23は、手順R42として、乱数 $R_A$ と $K_A$ を生成し、次に $V_A = K_A \cdot G$ の計算を行い、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、バージョンナンバー $\text{Rev}V_A$ からなるビット列にデジタル署名を行って $\text{Sig}_A$ を得、これら $R_A$ 、 $R_B$ 、 $V_A$ 、 $\text{Rev}V_A$ 、 $\text{Sig}_A$ とパブリック鍵証明書 $\text{Cert}_A$ をメモリ記録再生装置200に送る。なお、セキュリティモジュール23がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

上記セキュリティモジュール23から $\text{Cert}_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $\text{Rev}V_A$ 、 $\text{Sig}_A$ を受け取ると、メモリ記録再生装置200は、パブリック鍵証明書 $\text{Cert}_A$ の検証を行い、その検証をパスできないときには、そのセキュリティモジュール23を備えたメモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方、パブリック鍵証明書 $\text{Cert}_A$ の検証において正当であると判定された場合、上記パブリック鍵証明書 $\text{Cert}_A$ からパブリック鍵 $\text{PubKey}_A$ を手に入れる。次に、メモリ記録再生装置200は、セキュリティモジュール23から返送されてきた乱数 $R_B$ と、先の手順R41で生成した乱数 $R_B$ とが等しく、且つデジタル署名 $\text{Sig}_A$ が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジ

ジュール 23 を備えたメモリ情報記録媒体 20 が不正な媒体であると判断して当該プロトコルを終了する。

上記セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、メモリ記録再生装置 200 は、自己の不揮発性メモリ 210 に格納しているリボケーションリストを用い、セキュリティモジュール 23 を備えたメモリ情報記録媒体 20 の  $ID_A$  が当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記  $ID_A$  がリボケーションリストに掲載されている場合には、当該セキュリティモジュール 23 を備えたメモリ情報記録媒体 20 は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記  $ID_A$  が当該リボケーションリストに掲載されていない場合、メモリ記録再生装置 200 は、手順 R43 として、 $K_B$  を生成して  $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、バージョンナンバー  $RevV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。次にメモリ記録再生装置 200 は、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  とパブリック鍵証明書  $Cert_B$  を、セキュリティモジュール 23 に送る。なお、メモリ記録再生装置 200 がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 23 は、上記パブリック鍵証明書  $Cert_B$  の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置 200 を不正な装置とみなして当該プロトコルを終了し、一方、上記パブリック鍵証明書  $Cert_B$  の検

証において正当であると判定された場合は、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 23 は、メモリ記録再生装置 200 から返送されてきた乱数  $R_A$  と先に手順 R42 で生成した乱数  $R_A$  とが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 200 が不正な装置であると判断して当該プロトコルを終了する。

上記メモリ記録再生装置 200 から返送されてきた乱数  $R_A$  と先に生成したものが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたとき、セキュリティモジュール 23 は、自己の不揮発性メモリ 44 に格納しているリボケーションリストを用い、上記  $ID_B$  が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記  $ID_B$  がリボケーションリストに掲載されている場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。

一方、上記  $ID_B$  がリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 では  $K_A \cdot V_B$  の計算を行い、また、メモリ記録再生装置 200 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュリティモジュール 23 とメモリ記録再生装置 200 が共有する。

次に、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方

が新しい場合、手順 R 4 4 又は R 4 5 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、当該リボケーションリスト内に含まれるセンタ T C のデジタル署名 T C Sig を検証し、当該デジタル署名 T C Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新し、一方で、デジタル署名 T C Sig が正しくない場合は、当該プロトコルを終了する。

その後、メモリ記録再生装置 2 0 0 は、手順 R 4 6 として、メモリ情報記録媒体 2 0 のメモリ部 2 2 に記録するコンテンツデータを暗号化するための暗号鍵 K co を定め、この暗号鍵 K co をセッション鍵 K se にて暗号化した値 E nc (K se, K co) をセキュリティモジュール 2 3 に送信する。

この時のセキュリティモジュール 2 3 は、手順 R 4 7 として、上記メモリ記録再生装置 2 0 0 から送信されてきた値 E nc (K se, K co) をセッション鍵 K se を用いて復号して暗号鍵 K co を復元し、さらに、この暗号鍵 K co を自己のストレージ鍵 K st にて暗号化した値 E nc (K st, K co) をメモリ部 2 2 に格納し、或いは暗号鍵 K co を不揮発性メモリ 4 4 に格納する。

その後、メモリ記録再生装置 2 0 0 は、手順 R 4 8 として、上記暗号鍵 K co を用いて暗号化したコンテンツデータ E nc (K co, data) をセキュリティモジュール 2 3 に送る。

この時のセキュリティモジュール 2 3 は、手順 R 4 9 として、当該暗号化されているコンテンツデータ E nc (K co, data) をメモリ部 2 2 に格納する。

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

<第2の実施の形態の記録処理手順（詳細2）>

上記図16の例では、セキュリティモジュール23とメモリ記録再生装置200において、手順R42，R43のように、自己が保持しているリボケーションリスト内にそれぞれ相手方のIDが掲載されているか否かの検証を行った後、手順R44，R45にてリボケーションリストのバージョンナンバーの新旧をチェックし、新しいバージョンのリボケーションリストで古いバージョンのリボケーションリストを更新する例を挙げたが、以下に説明するように、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDが掲載されているか否かを検証するようにしてもよい。この場合、必ず新しいバージョンのリボケーションリストによって相手方のIDがチェックされるため、より確実に不正なものであるか否かを判定できる。なお、両者のリボケーションリストのバージョンナンバーが同じ場合もあり得るので、以下の説明では、バージョンナンバーが同じ場合も考慮して説明する。

図17には、第2の実施の形態において、上述のように先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示す。

なお、図17の手順R51乃至手順R56までは、前述した第1の実施の形態における図8の手順R21乃至手順R26までと略々同じである。



この図 17 において、メモリ記録再生装置 200 は、手順 R 5 1 として、乱数  $R_B$  を記録コマンドと共にセキュリティモジュール 23 に送る。上記記録コマンドと乱数  $R_B$  を受け取ったセキュリティモジュール 23 は、手順 R 5 2 として、乱数  $R_A$  と  $K_A$  を生成し、 $V_A = K_A \cdot G$  の計算を行い、さらに、前記同様に乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、バージョンナンバー  $RevV_A$  からなるビット列にデジタル署名を行って  $Sig_A$  を生成し、それら  $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $Sig_A$  とパブリック鍵証明書  $Cert_A$  をメモリ記録再生装置 200 に送る。

上記セキュリティモジュール 23 から  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $Sig_A$  を受け取ると、メモリ記録再生装置 200 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行う。すなわち、メモリ記録再生装置 200 は、パブリック鍵証明書  $Cert_A$  の検証を行い、当該検証をパスできないときには、そのセキュリティモジュール 23 を備えたメモリ情報記録媒体 20 を不正な媒体とみなして当該プロトコルを終了し、一方で、パブリック鍵証明書  $Cert_A$  の検証において正当であると判定された場合は、上記パブリック鍵証明書  $Cert_A$  からパブリック鍵  $PubKey_A$  を手に入れる。次に、メモリ記録再生装置 200 は、セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先の手順 R 5 1 で生成した乱数  $R_B$  とが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 23 を備えたメモリ情報記録媒体 20 が不正な媒体であると判断して当該プロトコルを終了する。

上記メモリ記録再生装置 200 から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判

定されたとき、メモリ記録再生装置 200 は、手順 R 5 3 として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、バージョンナンバー  $RevV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を生成し、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  とパブリック鍵証明書  $Cert_B$  をセキュリティモジュール 23 に送る。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 23 は、メモリ記録再生装置 200 のパブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。すなわち、セキュリティモジュール 23 は、先ず、パブリック鍵証明書  $Cert_B$  の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置 200 を不正な装置とみなして当該プロトコルを終了し、一方で、パブリック鍵証明書  $Cert_B$  の検証において正当であると判定された場合には、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 23 は、メモリ記録再生装置 200 から返送されてきた乱数  $R_A$  と先の手順 R 5 2 で生成した乱数  $R_A$  とが等しく、且つデジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 200 が不正な装置であると判断して当該プロトコルを終了する。

上述のように、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 では  $K_A \cdot V_B$  の計算を行い、また、メモリ記録再生装置 200 では  $K_B \cdot V_A$  の計算を行い、さらにそれらの  $x$  座標の下位  $z$  ビットをセッション鍵  $K_{se}$  としてこれらセキュ

リティモジュール 23 とメモリ記録再生装置 200 が共有する。

また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。当該相互検証の結果、両者において共にリボケーションリストに掲載されていないと判定された場合には、後段の手順 R56 の処理に進む。また、セキュリティモジュール 23 において、メモリ記録再生装置 200 の ID<sub>B</sub> が自己のリボケーションリストに掲載されている場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置 200 において、セキュリティモジュール 23 の ID<sub>A</sub> が自己のリボケーションリストに掲載されている場合には、当該セキュリティモジュール 23 は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール 23 とメモリ記録再生装置 200 においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R54 又は R55 として、上記新しいバージョンのリボケーションリストを

相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方のID検証を行うと共に、古いバージョンのリボケーションリストを更新する。

すなわち例えば、セキュリティモジュール23のリボケーションリストのバージョンが、メモリ記録再生装置200のものよりも新しい場合、セキュリティモジュール23では自己が保持するリボケーションリストを用いてメモリ記録再生装置200のID<sub>B</sub>の検証を行い、その検証の結果、メモリ記録再生装置200がリボケーションリストに記載されていないとき、手順R54として、自己が保持しているリボケーションリストをメモリ記録再生装置200に送る。当該リボケーションリストを受け取ったメモリ記録再生装置200は、当該送られてきた新しいリボケーションリストを用いてセキュリティモジュール23のID<sub>A</sub>の検証を行い、その検証の結果、セキュリティモジュール23のID<sub>A</sub>がリボケーションリストに記載されていないとき、上記セキュリティモジュール23から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタTCのデジタル署名TCSigを検証し、当該デジタル署名TCSigが正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、デジタル署名TCSigが正しくない場合は、当該プロトコルを終了する。

また、メモリ記録再生装置200のリボケーションリストのバージョンが、セキュリティモジュール23のものよりも新しい場合、メモリ記録再生装置200では自己が保持するリボケーションリストを用いてセキュリティモジュール23のID<sub>A</sub>の検証を行い、その

検証の結果、セキュリティモジュール 23 がリボケーションリストに記載されていないとき、手順 R 55 として、自己が保持しているリボケーションリストをセキュリティモジュール 23 に送る。当該リボケーションリストを受け取ったセキュリティモジュール 23 は、その送られてきた新しいリボケーションリストを用いてメモリ記録再生装置 200 の ID<sub>B</sub> の検証を行い、その検証の結果、メモリ記録再生装置 200 の ID<sub>B</sub> がリボケーションリストに記載されていないとき、上記メモリ記録再生装置 200 から送られてきた新しいバージョンのリボケーションリスト内に含まれるセンタ TC のデジタル署名 TC Sig を検証し、当該デジタル署名 TC Sig が正しい場合、そのリボケーションリストを用いて自己が保持している古いリボケーションリストを更新する。一方、デジタル署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

次に、メモリ記録再生装置 200 は、手順 R 56 として、メモリ情報記録媒体 20 のメモリ部 22 に記録するコンテンツデータを暗号化するための暗号鍵 K<sub>co</sub> をセッション鍵 K<sub>se</sub> にて暗号化した値 E<sub>nc</sub> (K<sub>se</sub>, K<sub>co</sub>) をセキュリティモジュール 23 に送信する。

この時のセキュリティモジュール 23 は、手順 R 57 として、上記メモリ記録再生装置 200 から送信されてきた値 E<sub>nc</sub> (K<sub>se</sub>, K<sub>co</sub>) をセッション鍵 K<sub>se</sub> を用いて復号することにより、暗号鍵 K<sub>co</sub> を復元し、さらに、この暗号鍵 K<sub>co</sub> を自己が持つストレージ鍵 K<sub>st</sub> にて暗号化した値 E<sub>nc</sub> (K<sub>st</sub>, K<sub>co</sub>) をメモリ部 22 或いは不揮発性メモリ 44 に格納する。

その後、メモリ記録再生装置 200 は、手順 R 58 として、上記暗号鍵 K<sub>co</sub> を用いて暗号化したコンテンツデータ E<sub>nc</sub> (K<sub>co</sub>, data)

をセキュリティモジュール 23 に送る。

この時のセキュリティモジュール 23 は、手順 R 59 として、当該暗号化されているコンテンツデータ  $Enc(Kco, data)$  をメモリ部 22 に格納する。なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

< 第 2 の実施の形態の記録処理手順（変形例） >

次に、この第 2 の実施の形態において、メモリ情報記録媒体 20 のメモリ部 22 へのデータの記録処理については、図 18 のようにすることも可能である。なお、図 18 の手順 R 61 乃至 R 64 については、図 15 の手順 R 31 乃至 R 34 と同じであるためその説明は省略する。

この図 18 の例において、メモリ記録再生装置 200 は、手順 R 65 として、前述の認証と鍵共有プロトコルにおいてセキュリティモジュール 23 と共有したセッション鍵  $Kse$  を用いてデータを暗号化し、当該暗号化されたデータ  $Enc(Kse, data)$  をセキュリティモジュール 23 に送る。

この暗号化されたデータ  $Enc(Kse, data)$  を受け取ったセキュリティモジュール 23 は、手順 R 66 として、同じくセッション鍵  $Kse$  を用いてこれを復号し、平文のデータを得、次に新たに発生させた暗号鍵  $Kco$  で暗号化した値  $Enc(Kco, data)$  をデータ用のメモリ部 22 に記録する。

ここで、セキュリティモジュール 23 は、暗号鍵  $Kco$  を安全にその内部の不揮発性メモリ 44 に格納するか、セキュリティモジュール 23 が予め格納しているストレージ鍵  $Kst$  を用いて暗号鍵  $Kco$  を暗号化した値  $Enc(Kst, Kco)$  を上記大容量のメモリ部 22 に格納

する。このようにすると、セキュリティモジュール 23 はデータの暗号鍵 Kco をメモリ記録再生装置 200 にも教えないで済む（つまり、外部に漏らさない）ようになる。

＜第 2 の実施の形態の再生処理手順＞

次に、図 19 乃至図 22 を用いて、上記第 2 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 20 のメモリ部 22 からデータを再生する手順を説明する。

なお、上述したように、第 2 の実施の形態のメモリ記録再生装置 200 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 210 に格納しており、また同様に、当該第 2 の実施の形態のメモリ情報記録媒体 20 のセキュリティモジュール 23 は、センタ TC から与えられた ID、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを上記不揮発性メモリ 44 に格納している。また、メモリ記録再生装置 200 は、再生すべきデータに付与されたレコーディング ID を知っているものとする。

先ず、図 19 において、メモリ記録再生装置 200 は、手順 P 31 として、メモリ情報記録媒体 20 のセキュリティモジュール 23 に対して、これからデータの再生を行うことを示す再生コマンド（再生開始コマンド）と、レコーディング ID とを送る。

次に、手順 P 32 として、メモリ記録再生装置 200 及びメモリ情報記録媒体 20 のセキュリティモジュール 23 は、上記再生コマンドをトリガーとして、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する。このプロトコルの内容は、前述した第 1

の実施の形態におけるデータの再生時に用いられるプロトコルと同様であり、それぞれ他方が持つパブリック鍵とプライベート鍵が正しいことの検証と、リボケーションリストに相手方のIDが載せられていないことの確認を互いに行い、セッション鍵 $K_{se}$ を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。

また、前記図15の手順R33, R34と同様に、図19の手順P33, P34として、どちらかが相対的に新しいリボケーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリボケーションリストを更新することも同様である。すなわち、手順P33には、セキュリティモジュール23上のリボケーションリストのバージョンが、メモリ記録再生装置200上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示しており、また、手順P34には、メモリ記録再生装置200上のリボケーションリストのバージョンが、セキュリティモジュール23上のリボケーションリストのバージョンよりも新しい場合におけるリボケーションリストの流れを示している。

なお、手順P33, P34におけるリボケーションリストの送付は、後の手順P35, P36におけるデータの再生と順序が前後してもかまわない。つまり、手順P35, P36にてデータの記録を行った後に、手順P33或いはP34でのリボケーションリストの送付を行うようにしてもよい。

次に、データをメモリ情報記録媒体20のメモリ部22から読み出す前に、このデータを暗号化したときの暗号鍵 $K_{co}$ をメモリ記録



再生装置 200 が知ることが必要になる。

暗号鍵  $K_{co}$  は、セキュリティモジュール 23 が安全にその内部の不揮発性メモリ 44 に格納しているか、或いはセキュリティモジュール 23 が予め格納しているストレージ鍵  $K_{st}$  を用いて当該暗号鍵  $K_{co}$  を暗号化した値  $Enc(K_{st}, K_{co})$  としてメモリ部 22 に記録されている。

前者の場合、セキュリティモジュール 23 は、不揮発性メモリ 44 に格納されている暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化した値  $Enc(K_{se}, K_{co})$  を、メモリ記録再生装置 200 に送る。メモリ記録再生装置 200 では、当該値  $Enc(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することにより暗号鍵  $K_{co}$  を得る。

一方、後者の場合、セキュリティモジュール 23 は、手順 P35 として、メモリ部 22 から上記ストレージ鍵  $K_{st}$  で暗号鍵  $K_{co}$  を暗号化した値  $Enc(K_{st}, K_{co})$  を読み出し、これをストレージ鍵  $K_{st}$  を用いて復号して暗号鍵  $K_{co}$  を得る。さらに、この暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化した値  $Enc(K_{se}, K_{co})$  を、手順 P36 としてメモリ記録再生装置 200 に送る。メモリ記録再生装置 200 は、当該値  $Enc(K_{se}, K_{co})$  をセッション鍵  $K_{se}$  を用いて復号することにより暗号鍵  $K_{co}$  を得る。

上述のように、メモリ記録再生装置 200 は、データを暗号化したときの暗号鍵  $K_{co}$  を得ることができる。

その後、メモリ記録再生装置 200 は、上記メモリ情報記録媒体 20 のメモリ部 22 から、上記暗号鍵  $K_{co}$  を用いて暗号化されているデータ  $Enc(K_{co}, data)$  を読み出し、先に取得した暗号鍵  $K_{co}$  を用いてこれを復号し使用する。

以上が、メモリ情報記録媒体20のメモリ部22からデータを読み出す処理の基本的な手順である。

<第2の実施の形態の再生処理手順(詳細1)>

次に、図20には、上記第2の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20からデータを再生するまでの手順の詳細を示す。なお、この図20では、メモリ記録再生装置200に係る各情報について「B」の文字を付し、メモリ情報記録媒体20のセキュリティモジュール23に係る各情報について「A」の文字を付している。上述同様に、メモリ記録再生装置200とセキュリティモジュール23は、センタTCから与えられたID(セキュリティモジュール23のID<sub>A</sub>、メモリ記録再生装置200のID<sub>B</sub>)、公開鍵暗号系のプライベート鍵、パブリック鍵、パブリック鍵証明書、及びリボケーションリストを、それぞれ対応する不揮発性メモリ210、44に格納している。

図20の手順P41乃至手順P46までは、前述した第1の実施の形態における図10の手順P11乃至手順P16までと略々同じである。

すなわち、メモリ記録再生装置200は、手順P41として乱数R<sub>B</sub>と再生コマンドをセキュリティモジュール23に送る。セキュリティモジュール23は、手順P42として、乱数R<sub>A</sub>とK<sub>A</sub>を生成し、 $V_A = K_A \cdot G$ の計算を行い、乱数R<sub>A</sub>、乱数R<sub>B</sub>、値V<sub>A</sub>、バージョンナンバーRevV<sub>A</sub>からなるビット列にデジタル署名を行ってSig<sub>A</sub>を得、これらにパブリック鍵証明書Cert<sub>A</sub>を加えてメモリ記録再生装置200に送る。なお、セキュリティモジュール23がリボケーションリストを持たない場合或いは使用しない場合は、当該バージョ

ンナンバーとして例えば0を用いる。

次に、メモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ の検証を行い、その検証をパスできないときには、そのメモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合、上記パブリック鍵証明書 $Cert_A$ からパブリック鍵 $PubKey_A$ を手に入れる。次に、メモリ記録再生装置200は、セキュリティモジュール23から返送されてきた乱数 $R_B$ と先の手順P41で生成した乱数 $R_B$ とが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたときには、次の処理に進み、そうでない場合には上記メモリ情報記録媒体20が不正な媒体であると判断して当該プロトコルを終了する。

上記セキュリティモジュール23から返送されたきた乱数 $R_B$ と先に生成したものとの等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、メモリ記録再生装置200は、自己が保持しているリボケーションリストを用い、上記メモリ情報記録媒体20の $ID_A$ が当該リボケーションリストに掲載されていないことを検証し、この検証の結果、上記 $ID_A$ がリボケーションリストに掲載されている場合には、当該メモリ情報記録媒体20は不正な媒体であると判定し、当該プロトコルを終了する。一方、上記 $ID_A$ が当該リボケーションリストに掲載されていない場合、メモリ記録再生装置200は、手順P43として、 $K_B$ を生成して $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、バージョンナンバー $RevV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得、それらにパブリック鍵証明書 $Cert_B$ を加えてセキュリティモジュール23に送る。なお、メモリ記録再生装置200がリボケーションリストを持たな

い場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

次に、セキュリティモジュール23は、上記パブリック鍵証明書 $Cert_B$ の検証を行い、当該検証をパスできないときには、そのメモリ記録再生装置200を不正な装置とみなして当該プロトコルを終了し、一方、当該検証において正当であると判定された場合は、上記パブリック鍵証明書 $Cert_B$ からパブリック鍵 $PubKey_B$ を手に入れる。次に、セキュリティモジュール23は、メモリ記録再生装置200から返送されてきた乱数 $R_A$ と先に手順P42で生成した乱数 $R_A$ とが等しく、且つデジタル署名 $Sig_B$ が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置200が不正な装置であると判断して当該プロトコルを終了する。

上記メモリ記録再生装置200から返送されてきた乱数 $R_A$ と先に生成したものとは等しく、且つデジタル署名 $Sig_B$ が正当であると判定されたとき、セキュリティモジュール23は、自己が保持するリボケーションリストを用い、上記 $ID_B$ が当該リボケーションリストに掲載されていないことを検証し、その検証の結果、上記 $ID_B$ がリボケーションリストに掲載されている場合には、当該メモリ記録再生装置200は不正な装置であると判定し、当該プロトコルを終了する。

一方、上記 $ID_B$ がリボケーションリストに掲載されていない場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200は、セッション鍵 $K_{se}$ を生成して共有する。

次に、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 P 44 又は P 45 として、その新しいバージョンのリボケーションリストを相手方に送る。このように、相手方から新しいバージョンナンバーのリボケーションリストが送られてきた方は、センタ TC のデジタル署名 TC Sig を検証し、当該デジタル署名 TC Sig が正しい場合、その新しいリボケーションリストを用いた更新を行い、一方で、デジタル署名 TC Sig が正しくない場合は、当該プロトコルを終了する。

次に、暗号鍵 Kco を暗号化した値 Enc (Kst, Kco) が、例えばメモリ情報記録媒体 20 のメモリ部 22 に格納されているとした場合は、セキュリティモジュール 23 は、手順 P 46 として、上記メモリ部 22 から上記読み出した値 Enc (Kst, Kco) をストレージ鍵 Kst を用いて復号して暗号鍵 Kco を得、さらに、この暗号鍵 Kco をセッション鍵 Kse で暗号化した値 Enc (Kse, Kco) を、手順 P 47 としてメモリ記録再生装置 200 に送る。メモリ記録再生装置 200 は、当該値 Enc (Kse, Kco) をセッション鍵 Kse を用いて復号することにより暗号鍵 Kco を得る。

その後、セキュリティモジュール 23 は、手順 P 48 として、暗号化されているコンテンツデータ Enc (Kco, data) をメモリ情報記録媒体 20 のメモリ部 22 から読み出し、このデータ Enc (Kco, data) をメモリ記録再生装置 200 に送信する。メモリ記録再生装置 200 では、先に取得した暗号鍵 Kco を用いて、上記データ Enc (Kco, data) を復号する。

なお、上記リボケーションリストの伝送は、上記コンテンツデータの伝送の合間、または終了後に行ってもよい。

<第2の実施の形態の再生処理手順（詳細2）>

次に、図21には、第2の実施の形態においてデータの再生を行う場合において、前記第1の実施の形態の図11の例と同様に、先にリボケーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリボケーションリストを用いて相手方のIDが掲載されているか否かを検証するようにしたときの手順を示す。

なお、図21の手順P51乃至手順P55までは、前述した第1の実施の形態における図11の手順P21乃至手順R25までと略々同じである。

この図21において、メモリ記録再生装置200は、手順P51として、乱数 $R_B$ を再生コマンドと共にセキュリティモジュール23に送る。上記再生コマンドと乱数 $R_B$ を受け取ったセキュリティモジュール23は、手順P52として、乱数 $R_A$ と $K_A$ を生成し、 $V_A = K_A \cdot G$ の計算を行い、さらに、前記同様に乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、バージョンナンバー $RevV_A$ からなるビット列にデジタル署名を行って $Sig_A$ を生成し、それら $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $Sig_A$ とパブリック鍵証明書 $Cert_A$ をメモリ記録再生装置200に送る。

上記セキュリティモジュール23から $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $Sig_A$ を受け取ると、メモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行う。上記パブリック鍵証明書 $Cert_A$ の検証をパスできないときには、メモリ記録再生装置200は、メモリ情報記録媒体20を不正な媒体とみなして当該プロトコルを終了し、一方で、当該検証において正当であると

判定された場合は上記パブリック鍵証明書  $Cert_A$  からパブリック鍵  $PubKey_A$  を手に入れる。次に、メモリ記録再生装置 200 は、セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先の手順 R51 で生成した乱数  $R_B$  とが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはセキュリティモジュール 23 を備えたメモリ情報記録媒体 20 が不正な媒体であると判断して当該プロトコルを終了する。

上記セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、メモリ記録再生装置 200 は、手順 P53 として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、バージョンナンバー  $RevV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を生成し、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  とパブリック鍵証明書  $Cert_B$  をセキュリティモジュール 23 に送る。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 23 は、メモリ記録再生装置 200 のパブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。上記パブリック鍵証明書  $Cert_B$  の検証をパスできないとき、セキュリティモジュール 23 は、そのメモリ記録再生装置 200 を不正な装置とみなして当該プロトコルを終了し、一方で、当該検証で正当であると判定した場合には、上記パブリック鍵証明書  $Cert_B$  からパブリック鍵  $PubKey_B$  を手に入れる。次に、セキュリティモジュール 23 は、メモリ記録再生装置 200 から返送されてきた乱数  $R_A$  と先の手順 R52 で生成した乱数  $R_A$  とが等しく、且つデ

ジタル署名  $Sig_B$  が正当であると判定されたときには、次の処理に進み、そうでない場合にはメモリ記録再生装置 200 が不正な装置であると判断して当該プロトコルを終了する。

上述のように、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者が共に正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、前記セッション鍵  $K_{se}$  を生成して共有する。

また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 213 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するリボケーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリボケーションリストに掲載されていないことを検証する。

一方、セキュリティモジュール 23 とメモリ記録再生装置 200 においてそれぞれ相手方が持っているリボケーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P54 又は P55 として、上記新しいバージョンのリボケーションリストを相手方に送り、この新しいバージョンのリボケーションリストを受け取った側では当該新しいバージョンのリボケーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのリボケーシ



ョンリストを更新する。

手順P 5 6乃至P 5 9は、図20の手順P 4 6乃至P 4 9と同じであるためその説明は省略する。

<第2の実施の形態の再生処理手順（変形例）>

次に、当該第2の実施の形態におけるデータ再生の手順として、図22に示すように、図18に示したデータ記録時の手順に準ずる手順を用いることも可能である。なお、図22の手順P 6 1乃至P 6 4については、図19の手順P 3 1乃至P 3 4と同じであるためその説明は省略する。

この図22の例において、セキュリティモジュール23は、手順P 6 5として、メモリ部22から読み取った前記暗号化されているコンテンツデータ  $E_{nc}(K_{co}, data)$  を、暗号鍵  $K_{co}$  を用いて復号し、その復号後のデータをセッション鍵  $K_{se}$  を用いて暗号化する。セキュリティモジュール23は、当該セッション鍵  $K_{se}$  を用いて暗号化されたコンテンツデータ  $E_{nc}(K_{se}, data)$  を、手順P 6 6として、メモリ記録再生装置200に送信する。

メモリ記録再生装置200は、上記データ  $E_{nc}(K_{se}, data)$  を、自己が保持するセッション鍵  $K_{se}$  にて復号する。これにより、メモリ記録再生装置200は、復号後のコンテンツデータを得る。

このようにすることで、セキュリティモジュール23はデータを暗号化している暗号鍵  $K_{co}$  をメモリ記録再生装置200に教える必要がなくなる（暗号鍵  $K_{co}$  が外部に出力することがなくなる）。

〔第3の実施の形態（IM2，Dev2）〕

以上説明した第1、第2の実施の形態では、プライベート鍵が露呈してしまった情報記録媒体或いは記録再生装置のID（リボーク

される機器又は媒体の I D ) のリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、正当な情報記録媒体或いは記録再生装置を示すレジストレーションリストを用いることで、上述同様に不正に情報が複製等されることを防止することも可能である。

すなわち、レジストレーションリストは、一般に登録リスト或いは正直者リストとも呼ばれ、システム全体若しくはその中の一部であるサブシステムにおいて、正当な情報記録媒体もしくは記録再生装置であるとセンタ T C が判断したもの（媒体若しくは装置）の I D をリストアップし、それにデジタル署名を施したものである。

当該レジストレーションリストは、図 2 3 に示すように、例えば単調増加する番号であって当該レジストレーションリストのバージョンを示すバージョンナンバーと、正当な情報記録媒体或いは記録再生装置の I D （登録された機器又は媒体の I D ）のリストと、センタ T C によるデジタル署名とからなるものである。このレジストレーションリストの登録は、一例として、あるホームネットワーク内の装置および記録媒体の I D を、そのネットワーク内の一つの装置がリストアップしてセンタ T C に送信し、センタ T C がこれらの全ての記録媒体及び装置が正当なものであると判断したとき、このリストに対しデジタル署名を付加して送り返し、これを受け取った装置がホームネットワーク内にこのリストを配布するようなことにより行われる。これにより、そのホームネットワーク内で信頼できる装置及び記録媒体全ての I D を各装置と記録媒体は知ることができるようになり、当該レジストレーションリストにリストアップされている I D を持つエンティティ（装置や媒体）のみを信用して

プロトコルを行うことが可能となる。言い換えれば、プライベート鍵が露呈してしまった記録媒体又は装置、及びそれを用いて不正に複製された記録媒体又は不正に製造された装置については、レジストレーションリストに掲載されないことになり、したがってそれら不正な装置や媒体をこのシステムから排除することが可能になる。また、記録再生装置を工場から出荷する際には、最新版のレジストレーションリストを不揮発性メモリに格納して出荷する。

以下、上記レジストレーションリストを使用した第3の実施の形態について説明する。

第3の実施の形態は、前述の第1の実施の形態で説明した光ディスク情報記録媒体10のセキュリティモジュール13の不揮発性メモリ34と、光ディスク記録再生装置100の不揮発性メモリ110に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第3の実施の形態における光ディスク情報記録媒体10、光ディスク記録再生装置100の構成は、前記図1乃至図3と同じであるため、それら構成についての説明は省略する。

#### <第3の実施の形態の記録処理手順>

図24から図26を用いて、第3の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10にデータを記録する手順を説明する。なお、図24乃至図26は、前記第1の実施の形態の図6乃至図8と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図6乃至図8とは異なる部分のみ説明する。

図24の手順R102は図6の手順R2と対応するが、この第3

の実施の形態の場合の手順 R 1 0 2 では、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 との間でレジストレーションリストのバージョンナンバーを交換する。

また、図 2 4 の手順 R 1 0 3 , R 1 0 4 は、図 6 の手順 R 3 , R 4 と対応するが、この第 3 の実施の形態の場合の手順 R 1 0 3 , R 1 0 4 では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジストレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

なお、手順 R 1 0 3 , R 1 0 4 におけるレジストレーションリストの送付は、後の手順 R 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 5 にてデータの記録を行った後に、手順 R 1 0 3 或いは R 1 0 4 でのレジストレーションリストの送付を行うようにしてもよい。

#### < 第 3 の実施の形態の記録処理手順（詳細 1） >

次に、図 2 5 には、上記図 2 4 に示した第 3 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録するまでの手順の詳細を示しており、前記図 7 と略々同様な手順となっている。

この図 2 5 において、手順 R 1 1 2（図 7 の手順 R 1 2 に対応）の際のセキュリティモジュール 1 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、

レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列  $R_A || R_B || V_A || RegV_A$  にデジタル署名の関数  $Sign$  を用いたデジタル署名を行い  $Sig_A = Sign(PriKey_A, R_A || R_B || V_A || RegV_A)$  を得る。セキュリティモジュール 13 は、これら  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RegV_A$ ,  $Sig_A$  にパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 100 に送る。なお、セキュリティモジュール 13 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RegV_A$ ,  $Sig_A$  を受け取った光ディスク記録再生装置 100 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュールから返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己の不揮発性メモリ 110 に格納しているレジストレーションリストを用い、光ディスク情報記録媒体 10 の  $ID_A$  が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体 10 の  $ID_A$  がレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体 10 は不正な媒体であると判定し、当該プロトコルを終了する。

一方、上記  $ID_A$  が当該レジストレーションリストに登録されており、その光ディスク情報記録媒体 10 が正当であると判断した場合、光ディスク記録再生装置 100 は、手順 R113 (図 7 の手順 R13 に対応) として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 100 が持つレジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列  $R_B ||$

$R_A || V_B || \text{Reg}V_B$ にデジタル署名を行って  $\text{Sig}_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || \text{Reg}V_B)$ を得る。光ディスク記録再生装置100は、これら  $R_B, R_A, V_B, \text{Reg}V_B, \text{Sig}_B$ にパブリック鍵証明書  $\text{Cert}_B$ を付け、セキュリティモジュール13に送る。なお、光ディスク記録再生装置100がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

上記光ディスク記録再生装置100から  $\text{Cert}_B, R_B, R_A, V_B, \text{Reg}V_B, \text{Sig}_B$ を受け取ると、セキュリティモジュール13は、パブリック鍵証明書  $\text{Cert}_B$ 、デジタル署名  $\text{Sig}_B$ 、 $\text{ID}_B$ の検証を行い、その検証をパスした時、自己の不揮発性メモリ34に格納しているレジストレーションリストを用い、光ディスク記録再生装置100の  $\text{ID}_B$ が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置100の  $\text{ID}_B$ がレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置100は不正な装置であると判定し、当該プロトコルを終了する。

一方、光ディスク記録再生装置100の  $\text{ID}_B$ が当該レジストレーションリストに登録されており、その光ディスク記録再生装置100が正当であると判断した場合、すなわち、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100はセッション鍵  $K_{se}$ を生成して共有する。

次に、セキュリティモジュール13と光ディスク記録再生装置1

00は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順R114又はR115（図7の手順R14，R15に対応）として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタTCのデジタル署名TCSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

その後の手順R16以降は、前記図7の場合と同様である。

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

### <第3の実施の形態の記録処理手順（詳細2）>

図26には、前記第1の実施の形態における図8の手順を、レジストレーションリストにも適用した例を示している。すなわち、図26は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のIDを検証するようにした場合の、データ記録時の手順を示している。

この図26において、手順R122（図8の手順R22に対応）の際のセキュリティモジュール13は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列 $R_A||R_B||V_A||RegV_A$ にデジタル署名を行って $Sig_A$ を得、これら $R_A$ 、 $R_B$ 、 $V_A$ 、 $RegV_A$ 、 $Sig_A$ にパブリック鍵証明書Cert

$A$ を付けて光ディスク記録再生装置100に送る。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RegV_A$ ,  $Sig_A$ を受け取った光ディスク記録再生装置100は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数  $R_B$ と先に生成したものが等しく、且つデジタル署名  $Sig_A$ が正当であると判定されたとき、手順R123（図8の手順R23に対応）として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置100が持つレジストレーションリストのバージョンナンバー  $RegV_B$ からなるビット列にデジタル署名を行って  $Sig_B$ を得る。光ディスク記録再生装置100は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $Sig_B$ にパブリック鍵証明書  $Cert_B$ を付け、セキュリティモジュール13に送る。

上記光ディスク記録再生装置100から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $Sig_B$ を受け取ると、セキュリティモジュール13は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ の検証を行い、その検証をパスした時、次の処理に進む。

上述のように、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、セッション鍵  $K_{se}$ を生成して共有する。

また、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、それぞれ相手方が持っているレジストレーションリストのバージョ



ンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 R 26 の処理に進む。また、セキュリティモジュール 13 において、光ディスク記録再生装置 100 の ID<sub>B</sub> が自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置 100 において、セキュリティモジュール 13 の ID<sub>A</sub> が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール 13 は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール 13 と光ディスク記録再生装置 100 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 124 又は R 125 (図 8 の手順 R 24, R 25 に対応) として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのレジストレーショ

ンリストを更新する。

その後の手順R 2 6以降は、前記図8の場合と同様である。

#### <第3の実施の形態の再生処理手順>

次に、図27乃至図29を用いて、上記第3の実施の形態の光ディスク記録再生装置100が光ディスク12からデータを再生する手順を説明する。なお、図27乃至図26は、前記第1の実施の形態の図9乃至図11と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図9乃至図11とは異なる部分のみ説明する。

図27において、光ディスク記録再生装置100とセキュリティモジュール13は、手順P102（図9の手順P2に対応）にて、レジストレーションリストに相手方のIDが載せられていることの確認を互いに行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

また、手順P103，P104（図9の手順P3，P4に対応）として、光ディスク記録再生装置100とセキュリティモジュール13は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジストレーションリストを更新することも前記図9の場合と同様である。

その後の手順P5以降は、前記図9の場合と同様である。

#### <第3の実施の形態の再生処理手順（詳細1）>

次に、図28には、上記図27に示した第3の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10からデータを再生するまでの手順の詳細を示している。なお、当該図28の

手順は、前記図 10 と略々同様な手順となっている。

この図 28 において、手順 P 1 1 2 (図 10 の手順 P 1 2 に対応) の際のセキュリティモジュール 13 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にデジタル署名を行い  $Sig_A$  を得る。セキュリティモジュール 13 は、これらにパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 100 に送る。なお、セキュリティモジュール 13 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取った光ディスク記録再生装置 100 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と先に生成したものとが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己の不揮発性メモリ 110 に格納しているレジストレーションリストを用い、光ディスク情報記録媒体 10 の  $ID_A$  が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク情報記録媒体 10 の  $ID_A$  がレジストレーションリストに登録されていない場合には、当該光ディスク情報記録媒体 10 は不正な媒体であると判定し、当該プロトコルを終了する。

一方、上記  $ID_A$  が当該レジストレーションリストに登録されており、その光ディスク情報記録媒体 10 が正当であると判断した場合、光ディスク記録再生装置 100 は、手順 P 1 1 3 (図 10 の手順 P 1 3 に対応) として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 100 のレジストレー

ションリストのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。光ディスク記録再生装置 100 は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 13 に送る。なお、光ディスク記録再生装置 100 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記光ディスク記録再生装置 100 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 13 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証を行い、その検証をパスした時、自己の不揮発性メモリ 34 に格納しているレジストレーションリストを用い、光ディスク記録再生装置 100 の  $ID_B$  が当該レジストレーションリストに登録されていることを検証する。この検証の結果、光ディスク記録再生装置 100 の  $ID_B$  がレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置 100 は不正な装置であると判定し、当該プロトコルを終了する。

一方、光ディスク記録再生装置 100 の  $ID_B$  が当該レジストレーションリストに登録されており、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわち、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 13 と光ディスク記録再生装置 1

00は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順P114又はP115（図10の手順P14，P15に対応）として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタTCのデジタル署名TCSigを検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

その後の手順P16以降は、前記図10の場合と同様である。

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

### <第3の実施の形態の再生処理手順（詳細2）>

図29には、前記第1の実施の形態における図11の手順を、レジストレーションリストにも適用した例を示している。すなわち、図29は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方のIDを検証するようにした場合の、データ再生時の手順を示している。

この図29において、手順P122（図11の手順P22に対応）の際のセキュリティモジュール13は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って $Sig_A$ を得、これらにパブリック鍵証明書 $Cert_A$ を付けて光ディスク記録再生装置100に送る。

それらを受け取った光ディスク記録再生装置100は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 $R_B$ と先に生成したものが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順P123（図11の手順P23に対応）として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、当該装置100が持つレジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得る。光ディスク記録再生装置100は、これら $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$ にパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール13に送る。上記光ディスク記録再生装置100から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$ を受け取ると、セキュリティモジュール13は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行い、その検証をパスした時、次の処理に進む。

セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、セッション鍵 $K_{se}$ を生成して共有する。また、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置100とセキュリティモジュール13は、それぞれが保持す

るレジストレーションリストを用いて相手方のIDの検証を行い、互いに相手方のIDがレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順P26の処理に進む。また、セキュリティモジュール13において、光ディスク記録再生装置100のID<sub>B</sub>が自己のレジストレーションリストに登録されていない場合には、当該光ディスク記録再生装置100は不正な装置であると判定し、当該プロトコルを終了する。同じく、光ディスク記録再生装置100において、セキュリティモジュール13のID<sub>A</sub>が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール13は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール13と光ディスク記録再生装置100においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順P124又はP125（図11の手順P24，P25に対応）として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方のID検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

その後の手順P26以降は、前記図11の場合と同様である。

〔第4の実施の形態（IM4，Dev4）〕

次に、本発明の第4の実施の形態について説明する。

第4の実施の形態は、前述の第2の実施の形態で説明したメモリ情報記録媒体20のセキュリティモジュール23の不揮発性メモリ44と、メモリ記録再生装置200の不揮発性メモリ210に、前記リボケーションリストに代えて上記レジストレーションリストを格納するようにした例である。当該第4の実施の形態におけるメモリ情報記録媒体20、メモリ記録再生装置200の構成は、前記図12乃至図14と同じであるため、それら構成についての説明は省略する。

#### <第4の実施の形態の記録処理手順>

図30乃至図33を用いて、第4の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20にデータを記録する手順を説明する。なお、図30乃至図33は、前記第2の実施の形態の図15乃至図18と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図15乃至図18とは異なる部分のみ説明する。

図30は前記図15と略々同様な手順を表しており、手順R132（図15の手順R32に対応）として、メモリ記録再生装置200とセキュリティモジュール23との間でレジストレーションリストのバージョンナンバーを交換する。

また、手順R133，R134（図15の手順R33，R34に対応）では、何れかの一方が他方のレジストレーションリストより新しいレジストレーションリストを持っていた場合、当該新しいレジストレーションリストを持っている方は自分のレジストレーションリストを他方に送る。一方、古いレジストレーションリストを持



っている方は、新しいレジストレーションリストを持っている方から、当該新しいレジストレーションリストを送ってもらい、その正当性を検証した後、自分が持つレジストレーションリストを、その送られてきた新しいレジストレーションリストに更新する。

なお、手順 R 1 3 3，R 1 3 4 におけるレジストレーションリストの送付は、後の手順 R 3 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 3 5 にてデータの記録を行った後に、手順 R 1 3 3 或いは R 1 3 4 でのレジストレーションリストの送付を行うようにしてもよい。

#### <第 4 の実施の形態の記録処理手順（詳細 1）>

次に、図 3 1 には、上記図 3 0 に示した第 4 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 にデータを記録するまでの手順の詳細を示しており、前記図 1 6 と略々同様な手順となっている。

この図 3 1 において、手順 R 1 4 2（図 1 6 の手順 R 4 2 に対応）の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にデジタル署名を行い  $Sig_A$  を得る。セキュリティモジュール 2 3 は、これらにパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 2 0 0 に送る。なお、セキュリティモジュール 2 3 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

それら  $Cert_A$ ， $R_A$ ， $R_B$ ， $V_A$ ， $RegV_A$ ， $Sig_A$  を受け取ったメモリ記録再生装置 2 0 0 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュ

リティモジュール 23 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己の不揮発性メモリ 210 に格納しているレジストレーションリストを用い、メモリ情報記録媒体 20 の  $ID_A$  が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体 20 の  $ID_A$  がレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体 20 は不正な媒体であると判定し、当該プロトコルを終了する。

一方、上記  $ID_A$  が当該レジストレーションリストに登録されており、そのメモリ情報記録媒体 20 が正当であると判断した場合、メモリ記録再生装置 200 は、手順 R143 (図 16 の手順 R43 に対応) として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 200 が持つレジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。メモリ記録再生装置 200 は、これらにパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 23 に送る。なお、メモリ記録再生装置 200 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 23 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証を行い、その検証をパスした時、自己の不揮発性メモリ 44 に格納しているレジストレーションリストを用い、メモリ記録再生装置 200 の  $ID_B$  が当該レジストレーションリストに登録されていることを検証する。

この検証の結果、メモリ記録再生装置 200 の ID<sub>B</sub> がレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。

一方、メモリ記録再生装置 200 の ID<sub>B</sub> が当該レジストレーションリストに登録されており、そのメモリ記録再生装置 200 が正当であると判断した場合、すなわち、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 はセッション鍵 K<sub>se</sub> を生成して共有する。

次に、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 R 144 又は R 145 (図 16 の手順 R 44, R 45 に対応) として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタ TC のデジタル署名 TC Sig を検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新 (リストのアップデート) する。

その後の手順 R 46 以降は、前記図 16 の場合と同様である。

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### < 第 4 の実施の形態の記録処理手順 (詳細 2) >

図 32 には、前記第 2 の実施の形態における図 17 の手順を、レ

ジストレーションリストにも適用した例を示している。すなわち、図 3 2 は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方の ID を検証するようにした場合の、データ記録時の手順を示している。

この図 3 2 において、手順 R 1 5 2 (図 1 7 の手順 R 5 2 に対応) の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にデジタル署名を行って  $Sig_A$  を得、これらにパブリック鍵証明書  $Cert_A$  を付けてメモリ記録再生装置 2 0 0 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取ったメモリ記録再生装置 2 0 0 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 1 5 3 (図 1 7 の手順 R 5 3 に対応) として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 2 0 0 が持つレジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。メモリ記録再生装置 2 0 0 は、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 2 3 に送る。

上記メモリ記録再生装置 2 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 2 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行い、その検証を

パスした時、次の処理に進む。

上述のように、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、セッション鍵  $K_{se}$  を生成して共有する。

また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 R56 の処理に進む。また、セキュリティモジュール 23 において、メモリ記録再生装置 200 の  $ID_B$  が自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該プロトコルを終了する。同じく、メモリ記録再生装置 200 において、セキュリティモジュール 23 の  $ID_A$  が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール 23 は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 1 5 4 又は R 1 5 5 (図 1 7 の手順 R 5 4, 5 5 に対応) として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

その後の手順 R 5 6 以降は、前記図 1 7 の場合と同様である。

#### < 第 4 の実施の形態の記録処理手順 (変形例) >

次に、この第 4 の実施の形態において、メモリ情報記録媒体 2 0 のメモリ部 2 2 へのデータの記録処理については、前述の図 1 8 と同様の図 3 3 に示すような手順とすることも可能である。

この図 3 3 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 R 1 6 2 (図 1 8 の手順 R 6 2 に対応) にて相互にレジストレーションリストのバージョンナンバーを交換する。

また、手順 R 1 6 3、R 1 6 4 (図 1 8 の手順 R 6 3, R 6 4 に対応) では、レジストレーションリストのバージョンナンバーが古い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

手順 R 6 5 以降の処理は、前記図 1 8 と同様である。

#### < 第 4 の実施の形態の再生処理手順 >

次に、図 3 4 乃至図 3 7 を用いて、上記第 4 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 のメモリ部 2 2 からデータを再生する手順を説明する。なお、図 3 4 乃至図 3 7 は、前記第 2 の実施の形態の図 1 9 乃至図 2 2 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 9 乃至図 2 2 とは異なる部分のみ説明する。

図 3 4 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 P 1 3 2 (図 1 9 の手順 P 3 2 に対応) にて、レジストレーションリストに相手方の ID が載せられていることの確認を互いに行い、自分が持つレジストレーションリストのバージョンナンバーを送り合う。

また、手順 P 1 3 3, P 1 3 4 (図 1 9 の手順 P 3 3, P 3 4 に対応) として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、どちらかが相対的に新しいレジストレーションリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のレジストレーションリストを更新することも同様である。

その後の手順 P 3 5 以降は、前記図 1 9 の場合と同様である。

#### < 第 4 の実施の形態の再生処理手順 (詳細 1) >

次に、図 3 5 には、上記図 2 0 に示した第 2 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 のメモリ部 2 2 からデータを再生するまでの手順の詳細を示している。なお、当該図 3 5 の手順は、前記図 2 0 と略々同様な手順となっている。

この図 3 5 において、手順 P 1 4 2 (図 2 0 の手順 P 4 2 に対応) の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  から

なるビット列にデジタル署名を行い  $Sig_A$  を得る。セキュリティモジュール 23 は、これらにパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 200 に送る。なお、セキュリティモジュール 23 がレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RegV_A$ ,  $Sig_A$  を受け取ったメモリ記録再生装置 200 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己が保持するレジストレーションリストを用い、メモリ情報記録媒体 20 の  $ID_A$  が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ情報記録媒体 20 の  $ID_A$  がレジストレーションリストに登録されていない場合には、当該メモリ情報記録媒体 20 は不正な媒体であると判定し、当該プロトコルを終了する。

一方、上記  $ID_A$  が当該レジストレーションリストに登録されており、そのメモリ情報記録媒体 20 が正当であると判断した場合、メモリ記録再生装置 200 は、手順 P143（図 20 の手順 P43 に対応）として、 $K_B$  の生成と  $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 200 のレジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。メモリ記録再生装置 200 は、これらにパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 23 に送る。なお、メモリ記録再生装置 200 がレジストレーションリストを持



たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

上記メモリ記録再生装置200から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RegV_B$ 、 $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ 、 $ID_B$ の検証を行い、その検証をパスした時、自己が保持するレジストレーションリストを用い、メモリ記録再生装置200の $ID_B$ が当該レジストレーションリストに登録されていることを検証する。この検証の結果、メモリ記録再生装置200の $ID_B$ がレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置200は不正な装置であると判定し、当該プロトコルを終了する。

一方、メモリ記録再生装置200の $ID_B$ が当該レジストレーションリストに登録されており、そのメモリ記録再生装置200が正当であると判断した場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200はセッション鍵 $K_{se}$ を生成して共有する。

次に、セキュリティモジュール23とメモリ記録再生装置200は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順P144又はP145（図20の手順P44，P45に対応）として、その新しいバージョンのレジストレーションリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのレジストレーションリストが送られてきた方は、当該レジストレーションリスト内に含まれるセンタTCのデジタル

署名  $TCSig$ を検証し、その検証をパスしたとき、その新しいレジストレーションリストを用いて自己が保持している古いレジストレーションリストを更新（リストのアップデート）する。

その後の手順 P 4 6 以降は、前記図 2 0 の場合と同様である。

なお、上記レジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### <第 4 の実施の形態の再生処理手順（詳細 2）>

図 3 6 には、前記第 2 の実施の形態における図 2 1 の手順を、レジストレーションリストにも適用した例を示している。すなわち、図 3 6 は、先にレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のレジストレーションリストを用いて相手方の ID を検証するようにした場合の、データ再生時の手順を示している。

この図 3 6 において、手順 P 1 5 2（図 2 1 の手順 P 5 2 に対応）の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、バージョンナンバー  $RegV_A$  からなるビット列にデジタル署名を行って  $Sig_A$  を得、これらにパブリック鍵証明書  $Cert_A$  を付けてメモリ記録再生装置 2 0 0 に送る。

それらを受け取ったメモリ記録再生装置 2 0 0 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 P 1 5 3（図 2 1 の手順 P 5 3 に対応）として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 2 0 0 が持つレジストレーションリス

トのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。メモリ記録再生装置 200 は、これらにパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 23 に送る。

上記メモリ記録再生装置 200 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 23 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行い、その検証をパスした時、次の処理に進む。

セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、セッション鍵  $K_{se}$  を生成して共有する。また、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行う。

両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するレジストレーションリストを用いて相手方の ID の検証を行い、互いに相手方の ID がレジストレーションリストに登録されていることを検証する。このレジストレーションリストの相互検証の結果、両者において共にレジストレーションリストに登録されていると判定された場合には、後段の手順 P 56 の処理に進む。また、セキュリティモジュール 23 において、メモリ記録再生装置 200 の  $ID_B$  が自己のレジストレーションリストに登録されていない場合には、当該メモリ記録再生装置 200 は不正な装置であると判定し、当該ブ

ロトコルを終了する。同じく、メモリ記録再生装置 200 において、セキュリティモジュール 23 の ID<sub>A</sub>が自己のレジストレーションリストに登録されていない場合には、当該セキュリティモジュール 23 は不正な媒体のものであると判定し、当該プロトコルを終了する。

一方、セキュリティモジュール 23 とメモリ記録再生装置 200 においてそれぞれ相手方が持っているレジストレーションリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 154 又は P 155 (図 21 の手順 P 54, P 55 に対応) として、上記新しいバージョンのレジストレーションリストを相手方に送り、この新しいバージョンのレジストレーションリストを受け取った側では当該新しいバージョンのレジストレーションリストを用いて相手方の ID 検証を行うと共に、古いバージョンのレジストレーションリストを更新する。

その後の手順 P 56 以降は、前記図 21 の場合と同様である。

#### < 第 4 の実施の形態の再生処理手順 (変形例) >

次に、この第 4 の実施の形態において、メモリ情報記録媒体 20 のメモリ部 22 からのデータの再生処理については、前述の図 22 と同様の図 37 に示すような手順とすることも可能である。

この図 37 において、メモリ記録再生装置 200 とセキュリティモジュール 23 は、手順 P 162 (図 22 の手順 P 62 に対応) にて相互にレジストレーションリストのバージョンナンバーを交換する。

また、手順 P 163、P 164 (図 22 の手順 P 63, P 64 に対応) では、レジストレーションリストのバージョンナンバーが古

い方を、新しいバージョンナンバーのレジストレーションリストにて更新する。

手順 P 6 5 以降の処理は、前記図 2 2 と同様である。

〔第 5 の実施の形態 (IM2, Dev2)〕

上述した第 1 及び第 2 の実施の形態ではリボケーションリストを、第 3 及び第 4 の実施の形態ではレジストレーションリストを用いて、不正に情報が複製等されることを防止した例を挙げたが、本発明では、これらリボケーションリストとレジストレーションリストを用いることで、さらに確実に不正な情報複製等を防止することも可能である。

ここで、リボケーションリストとレジストレーションリストを用いる場合、それら両者を同時に用いることも可能であり、或いは、それらのうち何れか一方を優先的に使用し、他方を使用しないようにすることも可能である。特に、上記何れか一方を優先的に使用する場合は、不正者リストであるリボケーションリストを優先することが望ましい。

また、両者を同時に用いる場合、それらリストを区別するために、例えば図 3 8 に示すようなリストフォーマットを用いることが可能である。すなわち、この図 3 8 のリストフォーマットは、リボケーションリストとレジストレーションリストの区別と、それらのバージョンナンバーと、上記区別がリボケーションリストの場合にはプライベート鍵が露呈してしまった情報記録媒体或いは記録再生装置の ID (リボークされる機器又は媒体の ID) のリスト、上記区別がレジストレーションリストの場合には正当な情報記録媒体或いは記録再生装置の ID (登録された機器又は媒体の ID) のリストと、

そしてセンタ T C によるデジタル署名とを含むものである。

上記リボケーションリストとレジストレーションリストを使用した第 5 の実施の形態について説明する。

第 5 の実施の形態は、前述の第 1 , 第 3 の実施の形態で説明した光ディスク情報記録媒体 1 0 のセキュリティモジュール 1 3 の不揮発性メモリ 3 4 と、光ディスク記録再生装置 1 0 0 の不揮発性メモリ 1 1 0 に、前記リボケーションリストとレジストレーションリストを格納するようにした例である。当該第 5 の実施の形態における光ディスク情報記録媒体 1 0 、光ディスク記録再生装置 1 0 0 の構成は、前記図 1 乃至図 3 と同じであるため、それら構成についての説明は省略する。

#### < 第 5 の実施の形態の記録処理手順 >

図 3 9 から図 4 1 を用いて、第 5 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録する手順を説明する。なお、図 3 9 乃至図 4 1 は、前記第 1 の実施の形態の図 6 乃至図 8 、第 3 の実施の形態の図 2 4 乃至図 2 6 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、それらとは異なる部分のみ説明する。

図 3 9 は前記図 6 , 図 2 4 と略々同様な手順を表しており、手順 R 2 0 2 ( 図 6 の手順 R 2 、図 2 4 の手順 R 1 0 2 に対応 ) として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 との間でリボケーションリスト及びレジストレーションリスト ( 以下、適宜、リストと呼ぶ ) のバージョンナンバーを交換する。

また、手順 R 2 0 3 , R 2 0 4 ( 図 6 の手順 R 3 , R 4 、図 2 4 の手順 R 1 0 3 , R 1 0 4 に対応 ) では、何れかの一方が他方のリ

ボケーションリスト及びレジストレーションリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

なお、手順 R 2 0 3, R 2 0 4 におけるリストの送付は、後の手順 R 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 5 にてデータの記録を行った後に、手順 R 2 0 3 或いは R 2 0 4 でのリストの送付を行うようにしてもよい。

#### < 第 5 の実施の形態の記録処理手順 (詳細 1) >

次に、図 4 0 には、上記図 3 9 に示した第 5 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 1 0 にデータを記録するまでの手順の詳細を示しており、前記図 7、図 2 5 と略々同様な手順となっている。

この図 4 0 において、手順 R 2 1 2 (図 7 の手順 R 1 2、図 2 5 の手順 R 1 1 2 に対応) の際のセキュリティモジュール 1 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、リボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列  $R_A || R_B || V_A || RevV_A || RegV_A$  にデジタル署名の関数  $Sign$  を用いたデジタル署名を行い  $Sig_A = Sign(PriKey_A, R_A || R_B || V_A || RevV_A || RegV_A)$  を得る。セキュリティモジュール 1 3 は、これら  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  にパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 1 0 0 に送る。なお、セキュリティモジュール 1 3 がリボケーションリスト又

はレジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして例えば0を用いる。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  を受け取った光ディスク記録再生装置100は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数  $R_B$  と先に生成したものが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己の不揮発性メモリ110に格納しているリボケーションリスト及びレジストレーションリストを用い、光ディスク情報記録媒体10の  $ID_A$  が当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク情報記録媒体10が不正な媒体であると判定した場合は、当該プロトコルを終了する。

一方、上記リストを用いた検証の結果、その光ディスク情報記録媒体10が正当であると判断した場合、光ディスク記録再生装置100は、手順R213（図7の手順R13、図25の手順R113に対応）として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置100が持つリボケーションリストのバージョンナンバー  $RevV_B$ 、レジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列  $R_B || R_A || V_B || RevV_B || RegV_B$  にデジタル署名を行って  $Sig_B = \text{Sign}(\text{PriKey}_B, R_B || R_A || V_B || RevV_B || RegV_B)$  を得る。光ディスク記録再生装置100は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  にパブ



リック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 13 に送る。  
なお、光ディスク記録再生装置 100 がリボケーションリスト又はレジストレーションリストを持たない場合或いは使用しない場合は、それぞれバージョンナンバーとして例えば 0 を用いる。

上記光ディスク記録再生装置 100 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 13 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証を行い、その検証をパスした時、自己の不揮発性メモリ 34 に格納しているリボケーションリスト及びレジストレーションリストを用い、光ディスク記録再生装置 100 の  $ID_B$  が当該リストに載っているか否かを検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、当該光ディスク記録再生装置 100 が不正な媒体であると判定した場合は、当該プロトコルを終了する。

一方、上記検証の結果、その光ディスク記録再生装置 100 が正当であると判断した場合、すなわち、セキュリティモジュール 13 と光ディスク記録再生装置 100 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 13 と光ディスク記録再生装置 100 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 13 と光ディスク記録再生装置 100 は、それぞれ相手方が持っているリボケーションリスト及びレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 R 214 又は R 215（図 7 の手順 R 14, R 15、図 25 の手順 R 114,

R 1 1 5 に対応) として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新 (リストのアップデート) する。

その後の手順 R 1 6 以降は、前記図 7, 図 2 5 の場合と同様である。

なお、上記リボケーションリスト及びレジストレーションリストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### < 第 5 の実施の形態の記録処理手順 (詳細 2) >

図 4 1 には、前記第 1 の実施の形態における図 8 や、第 3 の実施の形態における図 2 6 の手順を、本実施の形態のリボケーションリスト及びレジストレーションリストにも適用した例を示している。すなわち、図 4 1 は、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方の I D を検証するようにした場合の、データ記録時の手順を示している。

この図 4 1 において、手順 R 2 2 2 (図 8 の手順 R 2 2、図 2 6 の手順 R 1 2 2 に対応) の際のセキュリティモジュール 1 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、リボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列  $R_A || R_B || V_A || RevV_A || RegV_A$  にデジタル署名を行って  $Sig_A$  を得、これら  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  にパブリック鍵証明書  $Cert_A$  を付けて光ディスク記録再生装置

100に送る。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$ を受け取った光ディスク記録再生装置100は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数  $R_B$ と先に生成したもののが等しく、且つデジタル署名  $Sig_A$ が正当であると判定されたとき、手順R223（図8の手順R23、図26の手順R123に対応）として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置100が持つリボケーションリストのバージョンナンバー  $RevV_B$ 、レジストレーションリストのバージョンナンバー  $RegV_B$ からなるビット列にデジタル署名を行って  $Sig_B$ を得る。光ディスク記録再生装置100は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$ にパブリック鍵証明書  $Cert_B$ を付け、セキュリティモジュール13に送る。

上記光ディスク記録再生装置100から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$ を受け取ると、セキュリティモジュール13は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ の検証を行い、その検証をパスした時、次の処理に進む。

上述のように、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、セッション鍵  $K_{se}$ を生成して共有する。

また、セキュリティモジュール13と光ディスク記録再生装置100の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール13と光ディスク記録再生装置100は、

それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 100 とセキュリティモジュール 13 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方が正当であるか否か検証する。このときの検証は、上述したように両者のリストを用いても良いし、また、優先的に一方のリスト（特にリボケーションリスト）を用いても良い。この検証の結果、両者が共に正当であると判定された場合には、後段の手順 R 26 の処理に進む。また、セキュリティモジュール 13 において、光ディスク記録再生装置 100 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置 100 において、セキュリティモジュール 13 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

一方、セキュリティモジュール 13 と光ディスク記録再生装置 100 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 224 又は R 225（図 8 の手順 R 14，R 15、図 26 の手順 R 124，R 125 に対応）として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の ID 検証を行うと共に、古いバージョンのリストを更新する。

その後の手順 R 26 以降は、前記図 8、図 26 の場合と同様である。

<第5の実施の形態の再生処理手順>

次に、図42乃至図44を用いて、上記第5の実施の形態の光ディスク記録再生装置100が光ディスク12からデータを再生する手順を説明する。なお、図42乃至図44は、前記第1の実施の形態の図9乃至図11、第3の実施の形態の図27乃至図29と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図9乃至図11、図27乃至図29とは異なる部分のみ説明する。

図42において、光ディスク記録再生装置100とセキュリティモジュール13は、手順P202（図9の手順P2、図27の手順P102に対応）にて、リボケーションリスト及びレジストレーションリストを用い、互いに相手方が正当なものであることの確認を行い、自分が持つリストのバージョンナンバーを送り合う。

また、手順P203、P204（図9の手順P3、P4、図27の手順P103、P104に対応）として、光ディスク記録再生装置100とセキュリティモジュール13は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

その後の手順P5以降は、前記図9、図27の場合と同様である。

<第5の実施の形態の再生処理手順（詳細1）>

次に、図43には、上記図42に示した第5の実施の形態の光ディスク記録再生装置100が光ディスク情報記録媒体10からデータを再生するまでの手順の詳細を示している。なお、当該図43の手順は、前記図10、図28と略々同様な手順となっている。

この図43において、手順P212（図10の手順P12、図2

8の手順P 1 1 2に対応)の際のセキュリティモジュール1 3は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い $Sig_A$ を得る。セキュリティモジュール1 3は、これらにパブリック鍵証明書 $Cert_A$ を付け、光ディスク記録再生装置1 0 0に送る。なお、セキュリティモジュール1 3がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取った光ディスク記録再生装置1 0 0は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ 、 $ID_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール1 3から返送されてきた乱数 $R_B$ と先に生成したもののが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、自己の不揮発性メモリ1 1 0に格納しているリストを用い、光ディスク情報記録媒体1 0の $ID_A$ が正当であるか否かを検証する。この検証の結果、光ディスク情報記録媒体1 0の $ID_A$ が不正な媒体であると判定された場合は、当該プロトコルを終了する。

一方、光ディスク情報記録媒体1 0が正当であると判断した場合、光ディスク記録再生装置1 0 0は、手順P 2 1 3 (図1 0の手順P 1 3、図2 8の手順P 1 1 3に対応)として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、当該装置1 0 0のリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得る。光ディスク記録再生装

置 1 0 0 は、これら  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $RevV_B$ ,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 1 3 に送る。なお、光ディスク記録再生装置 1 0 0 がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記光ディスク記録再生装置 1 0 0 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 1 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証を行い、その検証をパスした時、自己の不揮発性メモリ 3 4 に格納しているリストを用い、光ディスク記録再生装置 1 0 0 が正当であるか否か検証する。この検証の結果、光ディスク記録再生装置 1 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。

一方、光ディスク記録再生装置 1 0 0 が正当であると判断した場合、すなわち、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 P 2 1 4 又は P 2 1 5 (図 1 0 の手順 P 1 4, P 1 5、図 2 8 の手順 P 1 1 4, P 1 1 5 に対応) として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含

まれるセンタTCのデジタル署名TCSigを検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

その後の手順P16以降は、前記図10、図28の場合と同様である。

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### <第5の実施の形態の再生処理手順（詳細2）>

図44には、前記第1の実施の形態における図11の手順、第3の実施の形態における図29の手順を、リボケーションリスト及びレジストレーションリストにも適用した例を示している。すなわち、図44は、先にリボケーションリスト及びレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合の、データ再生時の手順を示している。

この図44において、手順P222（図11の手順P22、図29の手順P122に対応）の際のセキュリティモジュール13は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って $Sig_A$ を得、これらにパブリック鍵証明書 $Cert_A$ を付けて光ディスク記録再生装置100に送る。

それらを受け取った光ディスク記録再生装置100は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱



数  $R_B$  と先に生成したものとが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 P 2 2 3 (図 1 1 の手順 P 2 3、図 2 9 の手順 P 1 2 3 に対応) として、 $K_B$  を生成し、 $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 1 0 0 が持つリボケーションリストのバージョンナンバー  $Rev V_B$ 、レジストレーションリストのバージョンナンバー  $Reg V_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。光ディスク記録再生装置 1 0 0 は、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $Reg V_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 1 3 に送る。上記光ディスク記録再生装置 1 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $Rev V_B$ 、 $Reg V_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 1 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行い、その検証をパスした時、次の処理に進む。

セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、セッション鍵  $K_{se}$  を生成して共有する。また、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

両者のバージョンナンバーが同じである場合、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 1 3 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方が正当であるか否かを検証する。このリストの相互検証の結果、両者にお

いて共に正当であると判定された場合には、後段の手順 P 2 6 の処理に進む。また、セキュリティモジュール 1 3 において、光ディスク記録再生装置 1 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、光ディスク記録再生装置 1 0 0 において、セキュリティモジュール 1 3 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

一方、セキュリティモジュール 1 3 と光ディスク記録再生装置 1 0 0 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 2 2 4 又は P 2 2 5 (図 1 1 の手順 P 2 4, P 2 5、図 2 9 の手順 P 1 2 4, P 1 2 5 に対応) として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の I D 検証を行うと共に、古いバージョンのリストを更新する。

その後の手順 P 2 6 以降は、前記図 1 1、図 2 9 の場合と同様である。

#### 〔第 6 の実施の形態 ( I M 4 , D e v 4 ) 〕

次に、本発明の第 6 の実施の形態について説明する。

第 6 の実施の形態は、前述の第 2, 第 4 の実施の形態で説明したメモリ情報記録媒体 2 0 のセキュリティモジュール 2 3 の不揮発性メモリ 4 4 と、メモリ記録再生装置 2 0 0 の不揮発性メモリ 2 1 0 に、前記リボケーションリストとレジストレーションリストの両方を格納するようにした例である。当該第 6 の実施の形態におけるメモリ情報記録媒体 2 0、メモリ記録再生装置 2 0 0 の構成は、前記

図 1 2 乃至図 1 4 と同じであるため、それら構成についての説明は省略する。

<第 6 の実施の形態の記録処理手順>

図 4 5 乃至図 4 8 を用いて、第 6 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 にデータを記録する手順を説明する。なお、図 4 5 乃至図 4 8 は、前記第 2 の実施の形態の図 1 5 乃至図 1 8、第 4 の実施の形態の図 3 0 乃至図 3 3 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 5 乃至図 1 8、図 3 0 乃至図 3 3 とは異なる部分のみ説明する。

図 4 5 は前記図 1 5、図 3 0 と略々同様な手順を表しており、手順 R 2 3 2 (図 1 5 の手順 R 3 2、図 3 0 の手順 R 1 3 2 に対応) として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。

また、手順 R 2 3 3、R 2 3 4 (図 1 5 の手順 R 3 3、R 3 4、図 3 0 の手順 R 1 3 3、R 1 3 4 に対応) では、何れかの一方が他方のリストより新しいリストを持っていた場合、当該新しいリストを持っている方は自分のリストを他方に送る。一方、古いリストを持っている方は、新しいリストを持っている方から、当該新しいリストを送ってもらい、その正当性を検証した後、自分が持つリストを、その送られてきた新しいリストに更新する。

なお、手順 R 2 3 3、R 2 3 4 におけるリストの送付は、後の手順 R 3 5 におけるデータの記録と順序が前後してもかまわない。つまり、手順 R 3 5 にてデータの記録を行った後に、手順 R 2 3 3 或

いはR 2 3 4でのリストの送付を行うようにしてもよい。

<第6の実施の形態の記録処理手順（詳細1）>

次に、図46には、上記図45に示した第6の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体20にデータを記録するまでの手順の詳細を示しており、前記図16、図31と略々同様な手順となっている。

この図46において、手順R 2 4 2（図16の手順R 4 2、図31に手順R 1 4 2に対応）の際のセキュリティモジュール23は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行い $Sig_A$ を得る。セキュリティモジュール23は、これらにパブリック鍵証明書 $Cert_A$ を付け、メモリ記録再生装置200に送る。なお、セキュリティモジュール23がリボケーションリスト又はレジストレーションリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

それら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取ったメモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ 、 $ID_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 $R_B$ と先に生成したもののが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、自己が保持しているリボケーションリスト及びレジストレーションリストを用い、メモリ情報記録媒体20が正当なものであるか否か検証する。この検証の結果、メモリ情報記録媒体20が不正な媒体であると判定された場合は、当該プロトコルを終了

する。

一方、上記メモリ情報記録媒体20が正当であると判断された場合、メモリ記録再生装置200は、手順R243（図16の手順R43、図31の手順R143に対応）として、 $K_B$ の生成と $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、当該装置200が持つリボケーションリストリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得る。メモリ記録再生装置200は、これらにパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。なお、メモリ記録再生装置200がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば0を用いる。

上記メモリ記録再生装置200から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ 、 $ID_B$ の検証を行い、その検証をパスした時、自己が保持するリボケーションリスト及びレジストレーションリストを用い、メモリ記録再生装置200が正当であるか否か検証する。この検証の結果、メモリ記録再生装置200が不正な装置であると判定された場合は、当該プロトコルを終了する。

一方、メモリ記録再生装置200が正当であると判断された場合、すなわち、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200はセッション鍵 $K_{se}$ を生成して共有する。

次に、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行い、自己の保持しているバージョンの方が新しい場合、手順 R 2 4 4 又は R 2 4 5（図 1 6 の手順 R 4 4，R 4 5、図 3 1 の手順 R 1 4 4，R 1 4 5 に対応）として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新（リストのアップデート）する。

その後の手順 R 4 6 以降は、前記図 1 6、図 3 1 の場合と同様である。

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

#### < 第 6 の実施の形態の記録処理手順（詳細 2） >

図 4 7 には、前記第 2 の実施の形態における図 1 7 の手順、第 4 の実施の形態における図 3 2 の手順を、リボケーションリスト及びレジストレーションリストにも適用した例を示している。すなわち、図 4 7 では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方の I D を検証するようにした場合の、データ記録時の手順を示している。

この図 4 7 において、手順 R 2 5 2（図 1 7 の手順 R 5 2、図 3 2 に手順 R 1 5 2 に対応）の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、リボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $Re$

$gV_A$ からなるビット列にデジタル署名を行って $Sig_A$ を得、これらにパブリック鍵証明書 $Cert_A$ を付けてメモリ記録再生装置200に送る。

これら $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$ を受け取ったメモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 $R_B$ と先に生成したもののが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順R253（図17の手順R53、図32の手順R153に対応）として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、当該装置200が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得る。メモリ記録再生装置200は、これら $R_B$ ,  $R_A$ ,  $V_B$ ,  $RegV_B$ ,  $RevV_B$ ,  $Sig_B$ にパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。

上記メモリ記録再生装置200から $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行い、その検証をパスした時、次の処理に進む。

上述のように、セキュリティモジュール23とメモリ記録再生装置200の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール23とメモリ記録再生装置200は、セッション鍵 $K_{se}$ を生成して共有する。

また、セキュリティモジュール23とメモリ記録再生装置200

の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、メモリ記録再生装置 200 とセキュリティモジュール 23 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方の ID がリストに登録されているか否かを検証する。このリストの相互検証の結果、両者において共に正当である、即ちリボケーションリストには登録されてなく且つレジストレーションリストに登録されている（リボケーションリストを優先させてもよい）と判定された場合には、後段の手順 R 56 の処理に進む。また、セキュリティモジュール 23 において、メモリ記録再生装置 200 が不正な装置であると判定された場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置 200 において、セキュリティモジュール 23 が不正な媒体のものであると判定された場合は、当該プロトコルを終了する。

一方、セキュリティモジュール 23 とメモリ記録再生装置 200 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 R 254 又は R 255

（図 17 の手順 R 54，R 55、図 32 の手順 R 154，R 155 に対応）として、上記新しいバージョンのリストを相手方に送り、この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方の ID 検証を行うと共に、古いバージョンのリストを更新する。



その後の手順 R 5 6 以降は、前記図 1 7、図 3 2 の場合と同様である。

<第 6 の実施の形態の記録処理手順（変形例）>

次に、この第 6 の実施の形態において、メモリ情報記録媒体 2 0 のメモリ部 2 2 へのデータの記録処理については、前述の図 1 8 や図 3 3 と同様の図 4 8 に示すような手順とすることも可能である。

この図 4 8 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 R 2 6 2（図 1 8 の手順 R 6 2、図 3 3 の手順 R 1 6 3 に対応）にて相互にリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。

また、手順 R 2 6 3、R 2 6 4（図 1 8 の手順 R 6 4、R 6 4、図 3 3 の手順 R 1 6 4、R 1 6 5 に対応）では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

手順 R 6 5 以降の処理は、前記図 1 8、図 3 3 と同様である。

<第 6 の実施の形態の再生処理手順>

次に、図 4 9 乃至図 5 2 を用いて、上記第 6 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ情報記録媒体 2 0 のメモリ部 2 2 からデータを再生する手順を説明する。なお、図 4 9 乃至図 5 2 は、前記第 2 の実施の形態の図 1 9 乃至図 2 2 や第 4 の実施の形態の図 3 4 乃至図 3 7 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 1 9 乃至図 2 2 や図 3 4 乃至図 3 7 とは異なる部分のみ説明する。

図 4 9 において、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、手順 P 2 3 2（図 1 9 の手順 P 3 2、図 3 4 の手順

P 1 3 2 に対応) にて、リボケーションリスト及びレジストレーションリストを用いて相手方の I D の正当性の確認を互いに行い、自分が持つリストのバージョンナンバーを送り合う。

また、手順 P 2 3 3, P 2 3 4 (図 1 9 の手順 P 3 3, P 3 4、図 3 4 の手順 P 1 3 3、P 1 3 4 に対応) として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、どちらかが相対的に新しいリストを持っていた場合には、それを他方に送り、送られた方はそれを用いて自分のリストを更新することも同様である。

その後の手順 P 3 5 以降は、前記図 1 9、図 3 4 の場合と同様である。

#### < 第 6 の実施の形態の再生処理手順 (詳細 1) >

次に、図 5 0 には、上記図 2 0 に示した第 2 の実施の形態や図 3 5 に示した第 4 の実施の形態のメモリ記録再生装置 2 0 0 がメモリ部 2 2 からデータを再生するまでの手順の詳細を示している。なお、当該図 5 0 の手順は、前記図 2 0, 図 3 5 と略々同様な手順となっている。

この図 5 0 において、手順 P 2 4 2 (図 2 0 の手順 P 4 2、図 3 5 の手順 P 1 4 2 に対応) の際のセキュリティモジュール 2 3 は、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、リボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にデジタル署名を行い  $Sig_A$  を得る。セキュリティモジュール 2 3 は、これらにパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 2 0 0 に送る。なお、セキュリティモジュール 2 3 がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$ を受け取ったメモリ記録再生装置 200 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$ 、 $ID_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 23 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、自己が保持するリストを用い、メモリ情報記録媒体 20 が正当であるか否かの検証を行う。この検証の結果、メモリ情報記録媒体 20 が不正な媒体であると判定した場合は、当該プロトコルを終了する。

一方、上記メモリ情報記録媒体 20 が正当であると判断した場合、メモリ記録再生装置 200 は、手順 P 243 (図 20 の手順 P 43、図 35 の手順 P 143 に対応) として、 $K_B$  の生成と  $V_B = K_B \cdot G$  の計算を行い、更に、上記乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、当該装置 200 のレジストレーションリストのバージョンナンバー  $RevV_B$ 、レジストレーションリストのバージョンナンバー  $RegV_B$  からなるビット列にデジタル署名を行って  $Sig_B$  を得る。メモリ記録再生装置 200 は、これらにパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 23 に送る。なお、メモリ記録再生装置 200 がリストを持たない場合或いは使用しない場合は、当該バージョンナンバーとして例えば 0 を用いる。

上記メモリ記録再生装置 200 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  を受け取ると、セキュリティモジュール 23 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$ 、 $ID_B$  の検証を行い、その検証をパスした時、自己が保持するリストを用い、メモリ記録再生装置 200 が正当であるか否かを検証する。この検証

の結果、メモリ記録再生装置 200 が不正な装置であると判定した場合は、当該プロトコルを終了する。

一方、メモリ記録再生装置 200 が正当であると判断した場合、すなわち、セキュリティモジュール 23 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 23 とメモリ記録再生装置 200 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 23 とメモリ記録再生装置 200 は、それぞれ相手方が持っているリボケーションリスト及びレジストレーションリストのバージョンナンバーのチェックを行い、自己の保持しているリストのバージョンの方が新しい場合、手順 P 244 又は P 245（図 20 の手順 P 44、P 45、図 35 の手順 P 144、P 145 に対応）として、その新しいバージョンのリストを相手方に送る。上述のように、相手方から新しいバージョンナンバーのリストが送られてきた方は、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig を検証し、その検証をパスしたとき、その新しいリストを用いて自己が保持している古いリストを更新する。

その後の手順 P 46 以降は、前記図 20、図 35 の場合と同様である。

なお、上記リストの伝送は、コンテンツデータの伝送の合間、または終了後に行ってもよい。

< 第 6 の実施の形態の再生処理手順（詳細 2） >

図 51 には、前記第 2 の実施の形態における図 21 や第 4 の実施の形態における図 36 の手順を、リボケーションリスト及びレジストレーションリストにも適用した例を示している。すなわち、図 5

1は、先にリボケーションリスト及びレジストレーションリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合の、データ再生時の手順を示している。

この図51において、手順P252（図21の手順P53、図36の手順P152に対応）の際のセキュリティモジュール23は、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、リボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストバージョンナンバー $RegV_A$ からなるビット列にデジタル署名を行って $Sig_A$ を得、これらにパブリック鍵証明書 $Cert_A$ を付けてメモリ記録再生装置200に送る。

それらを受け取ったメモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 $R_B$ と先に生成したものが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順P253（図21の手順P53、図36の手順P153に対応）として、 $K_B$ を生成し、 $V_B = K_B \cdot G$ の計算を行い、更に、上記乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、当該装置200が持つリボケーションリストのバージョンナンバー $RevV_B$ 、レジストレーションリストのバージョンナンバー $RegV_B$ からなるビット列にデジタル署名を行って $Sig_B$ を得る。メモリ記録再生装置200は、これらにパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。

上記メモリ記録再生装置200から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行い、

その検証をパスした時、次の処理に進む。

セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、セッション鍵  $K_{se}$  を生成して共有する。また、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 は、それぞれ相手方が持っているリストのバージョンナンバーのチェックを行う。

両者のバージョンナンバーが同じである場合、メモリ記録再生装置 2 0 0 とセキュリティモジュール 2 3 は、それぞれが保持するリストを用いて相手方の ID の検証を行い、互いに相手方が正当であるか否かの検証を行う。このリストの相互検証の結果、両者において共に正当であると判定された場合は、後段の手順 P 5 6 の処理に進む。また、セキュリティモジュール 2 3 において、メモリ記録再生装置 2 0 0 が不正な装置であると判定した場合は、当該プロトコルを終了する。同じく、メモリ記録再生装置 2 0 0 において、セキュリティモジュール 2 3 が不正な媒体のものであると判定した場合は、当該プロトコルを終了する。

一方、セキュリティモジュール 2 3 とメモリ記録再生装置 2 0 0 においてそれぞれ相手方が持っているリストのバージョンナンバーのチェックを行った結果、何れか一方の保持しているバージョンよりも他方のバージョンが新しい場合、手順 P 2 5 4 又は P 2 5 5 (図 2 1 の手順 P 5 4, P 5 5、図 3 6 の手順 P 1 5 4, P 1 5 5 に対応) として、上記新しいバージョンのリストを相手方に送り、

この新しいバージョンのリストを受け取った側では当該新しいバージョンのリストを用いて相手方のID検証を行うと共に、古いバージョンのリストを更新する。

その後の手順P56以降は、前記図21、図36の場合と同様である。

#### <第6の実施の形態の再生処理手順（変形例）>

次に、この第6の実施の形態において、メモリ情報記録媒体20のメモリ部22からのデータの再生処理については、前述の図22や図37と同様の図52に示すような手順とすることも可能である。

この図52において、メモリ記録再生装置200とセキュリティモジュール23は、手順P262（図22の手順P62、図37の手順P162に対応）にて相互にリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。

また、手順P263、P264（図22の手順P63、P64、図37の手順P163、P164に対応）では、リストのバージョンナンバーが古い方を、新しいバージョンナンバーのリストにて更新する。

手順P65以降の処理は、前記図22、図37と同様である。

なお、上述した本発明の各実施の形態では、一つの不揮発性メモリにリストを格納する例を挙げているが、もちろん2以上の不揮発性メモリにリストを格納しても、また一つの不揮発性メモリ内の一部の領域にリストを格納するようにしても良い。さらに、情報記録媒体内に設けられる不揮発性メモリは、セキュリティモジュールの外に配置されるものであってもよい。言い換えると、上述した各実施の形態において、リストを格納するための不揮発性メモリとは、

前記暗号化されたコンテンツデータを記録する領域（前記光ディスク 12 のデータ記憶領域や、メモリ部 22）以外の記憶領域であって、上記リストを記憶するために特に設けられた記憶領域のことを意味しており、パブリック鍵やプライベート鍵を保持する記憶領域とは異なっている。

〔媒体タイプと装置タイプの組み合わせに応じた実施の形態の説明〕

ところで、上述した第 1 乃至第 6 の実施の形態では、記録再生装置（100、200）が不揮発性メモリ（110、210）を備え、情報記録媒体のセキュリティモジュール（13、23）が不揮発性メモリ（34、44）を備え、これら不揮発性メモリにリボケーションリスト及び／又はレジストレーションリストを格納している例について説明したが、それら記録再生装置と情報記録媒体の何れか一方或いは両方において、リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えていない場合も考えられる。すなわち、リストを格納するための不揮発性メモリを備えることは、コストの上昇に繋がるため、当該不揮発性メモリを備えない記録再生装置や情報記録媒体、或いはプライベート鍵やパブリック鍵は記憶できるが、リストの情報については記憶できるだけの十分な記憶容量を持たない安価な不揮発性メモリしか備えていない記録再生装置や情報記録媒体が存在することが考えられる。

ここで、リボケーションリスト及び／又はレジストレーションリストを十分に格納できる不揮発性メモリを備えるか否かにより、上記情報記録媒体は以下に説明する第 1、第 2 の媒体タイプに分類す



ることができ、また、上記記録再生装置は、以下の第 1、第 2 の装置タイプに分類することができる。

第 1 の媒体タイプは、情報記録媒体が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えておらず、これらリストを当該情報記録媒体のコンテンツデータ記録用の領域に格納するようにした場合である。なお、第 1 の媒体タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

第 2 の媒体タイプは、情報記録媒体が上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

第 1 の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えていない場合である。なお、第 1 の装置タイプには、上記不揮発性メモリが上記リストを格納するのに十分な記憶容量を有していない場合も含む。

第 2 の装置タイプは、記録再生装置が、上記リボケーションリスト及び／又はレジストレーションリストを格納するための不揮発性メモリを備えている場合である。

なお、以下の説明では、上記第 1 の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプ I M 1 とし、上記第 2 の媒体タイプに相当する光ディスク情報記録媒体をメディアタイプ I M 2 とし、上記第 1 の媒体タイプに相当するメモリ情報記録媒体をメディアタイプ I M 3 とし、上記第 2 の媒体タイプに相当するメモリ情報記録媒体をメディアタイプ I M 4 と呼ぶことにする。さらに、上記

第 1 の装置タイプに相当する光ディスク記録再生装置をデバイスタイプ D e v 1 とし、上記第 2 の装置タイプに相当する光ディスク記録再生装置をデバイスタイプ D e v 2 とし、上記第 1 の装置タイプに相当するメモリ記録再生装置をデバイスタイプ D e v 3 とし、上記第 2 の装置タイプに相当するメモリ記録再生装置をデバイスタイプ D e v 4 とする。

図 5 3 には、当該メディアタイプ I M 1 に相当する光ディスク情報記録媒体 5 0 の概略構成を示す。この図 5 3 に示すメディアタイプ I M 1 の光ディスク情報記録媒体 5 0 は、図 5 4 に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール 5 3 を備えている。ただし、この図 5 4 に示すようにリストを格納するための不揮発性メモリを持たないセキュリティモジュール 5 3 であっても、プライベート鍵、パブリック鍵証明書、I D、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図 5 4 のセキュリティモジュール 5 3 は、それらプライベート鍵、パブリック鍵証明書、I D、バージョンナンバーを記憶するための不揮発性の鍵メモリ 3 6 を備えている。なお、図 5 3、図 5 4 における各部の構成は、前述の図 1、図 2 の例と同じであるため、それらの説明は省略する。

また、図 5 5 には、上記メディアタイプ I M 3 に相当するメモリ情報記録媒体 6 0 の概略構成を示す。この図 5 5 に示すメディアタイプ I M 3 のメモリ情報記録媒体 6 0 は、図 5 6 に示すように、リストを格納するための不揮発性メモリを持たないセキュリティモジュール 6 3 を備えている。ただし、この図 5 6 に示すようにリストを格納するための不揮発性メモリを持たないセキュリティモジュール

ル 6 3 であっても、プライベート鍵、パブリック鍵証明書、ID、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図 5 6 のセキュリティモジュール 6 3 は、それらプライベート鍵、パブリック鍵証明書、ID、バージョンナンバーを記憶するための不揮発性の鍵メモリ 4 7 を備えている。なお、これら図 5 5、図 5 6 における各部の構成は前述の図 1 2、図 1 3 の例と同じであるため、それらの説明は省略する。

以下、上記メディアタイプIM1とデバイスタイプDev1の組み合わせ(IM1, Dev1)、メディアタイプIM1とデバイスタイプDev2の組み合わせ(IM1, Dev2)、メディアタイプIM2とデバイスタイプDev1の組み合わせ(IM2, Dev1)、メディアタイプIM3とデバイスタイプDev3の組み合わせ(IM3, Dev3)、メディアタイプIM3とデバイスタイプDev4の組み合わせ(IM3, Dev4)、メディアタイプIM4とデバイスタイプDev3の組み合わせ(IM4, Dev3)のそれぞれについて、データ記録時と再生時の手順の説明を行う。なお、メディアタイプIM2とデバイスタイプDev2との組み合わせ(IM2, Dev2)は、前述した第1、第3、第5の実施の形態に相当し、メディアタイプIM4とデバイスタイプDev4との組み合わせ(IM4, Dev4)は前述した第2、第4、第6の実施の形態に相当するため、これらの組み合わせについての説明は省略する。

なお、以下の説明では、前述した第5、第6の実施の形態のように、リストとしてリボケーションリストとレジストレーションリストの両方を利用可能とした例を挙げて説明しているが、前述の第1

乃至第4の実施の形態のように何れか一方のリストのみ使用する場合であっても良いことは言うまでもない。また、以下の各実施の形態の説明では、先にリストのバージョンナンバーの新旧をチェックし、バージョンの新しい方のリストを用いて相手方のIDを検証するようにした場合を例に挙げており、前述の第1乃至第6の実施の形態にて説明した全ての手順に対応する説明は行わないが、以下の各実施の形態においても前記第1乃至第6の実施の形態にて説明した全ての手順と同様の手順で処理を行うことは可能である。

〔第7の実施の形態（IM1，Dev1）〕

先ず、第7の実施の形態として、メディアタイプIM1とデバイスタイプDev1の組み合わせ（IM1，Dev1）から説明する。

当該第7の実施の形態の組み合わせにおけるシステム構成は、図57に示すようになる。すなわち、デバイスタイプDev1の光ディスク記録再生装置300はリストを格納するための専用の不揮発性メモリを備えておらず（或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する）、また、メディアタイプIM1の光ディスク情報記録媒体50のセキュリティモジュール53はリストを格納するための不揮発性メモリを備えていない

（或いはリストを記憶できる十分な記憶容量を備えていない不揮発性メモリのみ有する）。ただし、この図57に示すようにリストを格納するための専用の不揮発性メモリを持たない光ディスク記録再生装置300であっても、プライベート鍵、パブリック鍵証明書、ID、バージョンナンバーを記憶するためのメモリは必要であり、したがって、当該図57の光ディスク記録再生装置300は、それらプライベート鍵、パブリック鍵証明書、ID、バージョンナンバ

ーを記憶するための不揮発性の鍵メモリ 1 1 1 を備えている。なお、当該図 5 7 における各部の構成は、前述の図 3 の例と同じであるため、それらの説明は省略する。

<第 7 の実施の形態の記録処理手順>

図 5 8 には、当該第 7 の実施の形態のメディアタイプ I M 1 とデバイスタイプ D e v 1 の組み合わせ ( I M 1 , D e v 1 ) の場合に、光ディスク記録再生装置 3 0 0 が光ディスク情報記録媒体 5 0 にデータを記録する手順を説明する。なお、図 5 8 において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

図 5 8 は前記図 3 9 と略々同様な手順を表しており、手順 R 3 0 2 (図 3 9 の手順 R 2 0 2 に対応) として、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。ここで、当該第 7 の実施の形態の場合、光ディスク記録再生装置 3 0 0 はリストを持たないため、手順 R 3 0 2 として、バージョンナンバー「0」をセキュリティモジュール 5 3 に送り、一方、セキュリティモジュール 5 3 は、光ディスク 1 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストのバージョンナンバーを、鍵メモリ 3 6 から読み出して光ディスク記録再生装置 3 0 0 に送ることになる。

次に、光ディスク記録再生装置 3 0 0 は、手順 R 3 0 3 として、光ディスク情報記録媒体 5 0 の光ディスク 1 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストを読み出す。

当該光ディスク記録再生装置 300 は、上記光ディスク情報記録媒体 50 の光ディスク 12 のコンテンツデータ記録用の領域から読み出したリストを用いて、当該光ディスク情報記録媒体 50 が正当なものであるか否か検証し、その検証の結果、当該光ディスク情報記録媒体 50 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 50 が正当であると判定した場合は、手順 R 304 として、上記リストをセキュリティモジュール 53 に送る。

セキュリティモジュール 53 は、当該リストを用いて、光ディスク記録再生装置 300 が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

上記セキュリティモジュール 53 が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置 300 とセキュリティモジュール 53 の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 5 に進むことになる。

#### < 第 7 の実施の形態の記録処理手順（詳細） >

次に、図 59 には、上記図 58 に示した第 7 の実施の形態の光ディスク記録再生装置 300 が光ディスク情報記録媒体 50 にデータを記録するまでの手順の詳細を示しており、前記図 40 と略々同様な手順となっている。

この図 59 において、セキュリティモジュール 53 は、手順 R 312（図 40 の手順 R 212 に対応）として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、鍵メモリ 36 に格納されているリストのバージョンナンバー  $RevV_A$ 、 $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を

付け、光ディスク記録再生装置 300 に送る。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  を受け取った光ディスク記録再生装置 300 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 53 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 313 として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ ,  $R_A$ ,  $V_B$ , 0, 0,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 53 に送る。

上記光ディスク記録再生装置 300 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ , 0, 0,  $Sig_B$  を受け取ると、セキュリティモジュール 53 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 53 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 300 とセキュリティモジュール 53 の両方で検証をパスしたとき、セキュリティモジュール 53 と光ディスク記録再生装置 300 はセッション鍵  $K_{se}$  を生成して共有する。

次に、光ディスク記録再生装置 300 は、手順 R 314 として、光ディスク 12 のデータ記録領域に格納されているリボケーションリスト及びレジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順 R 312 で取得したバージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いて

光ディスク情報記録媒体 50 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、光ディスク情報記録媒体 50 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 300 は、手順 R 315 として、そのリストをセキュリティモジュール 53 に送る。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーがセキュリティモジュール 53 の鍵メモリ 36 内に記憶されている前記バージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 300 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、光ディスク 12 が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 300 とセキュリティモジュール 53 の両方において正当であると判定した場合は、後段の手順 R 16 以降のデータ暗号化及び記録の処理に進むことになる。

#### <第 7 の実施の形態の再生処理手順>

次に、図 60 には、上記第 7 の実施の形態の光ディスク記録再生装置 300 が光ディスク 12 からデータを再生する手順を説明する。なお、図 60 の手順は、前記図 43 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 43 と



は異なる部分のみ説明する。

この図60において、セキュリティモジュール53は、手順P312（図43の手順P212に対応）として、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、鍵メモリ36に記録されているリストのバージョンナンバー $RevV_A$ 、 $RegV_A$ からなるビット列にパブリック鍵証明書 $Cert_A$ を付け、光ディスク記録再生装置300に送る。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取った光ディスク記録再生装置300は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール53から返送されてきた乱数 $R_B$ と先に生成したもののが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順P313（図43の手順P213に対応）として、乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、自己がリストを持たないことを示す

「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$ にパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール53に送る。

上記光ディスク記録再生装置300から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$ を受け取ると、セキュリティモジュール53は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール53にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置300とセキュリティモジュール53の両方で検証をパスしたとき、セキュリティモジュール53と光ディスク記録再生装置300はセッション鍵 $K_{se}$ を生成して共有する。

次に、光ディスク記録再生装置 3 0 0 は、手順 P 3 1 4 として、光ディスク 1 2 のデータ記録領域に格納されているリボケーションリスト及びレジストレーションリストを読み取り、そのリストのバージョンナンバーが先の手順 P 3 1 2 で取得したバージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 5 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、光ディスク情報記録媒体 5 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 3 0 0 は、手順 P 3 1 5 として、そのリストをセキュリティモジュール 5 3 に送る。なお、セキュリティモジュール 5 3 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったセキュリティモジュール 5 3 は、そのリストのバージョンナンバーが前記バージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 3 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、光ディスク 1 2 が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 5 3 の両方において正当であると判定した場合は、後段の手順 P 1 6 以降のデータ再生及び復号処理等に進むことになる。

〔第 8 の実施の形態（IM1 / Dev2）〕

次に、第 8 の実施の形態として、メディアタイプ I M 1 とデバイスタイプ D e v 2 の組み合わせ ( I M 1 , D e v 2 ) について説明する。

当該第 8 の実施の形態の組み合わせにおけるシステム構成は、図 6 1 に示すようになる。すなわち、デバイスタイプ D e v 2 の光ディスク記録再生装置 1 0 0 はリストを格納するための専用の前記不揮発性メモリ 1 1 0 を備えており、一方、メディアタイプ I M 1 の光ディスク情報記録媒体 5 0 のセキュリティモジュール 5 3 はリストを格納するための不揮発性メモリを備えていない。なお、当該図 6 1 における各部の構成は、前述の図 3 の例と同じであるため、それらの説明は省略する。

#### < 第 8 の実施の形態の記録処理手順 >

図 6 2 には、当該第 8 の実施の形態のメディアタイプ I M 1 とデバイスタイプ D e v 2 の組み合わせ ( I M 1 , D e v 2 ) の場合に、光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 5 0 にデータを記録する手順を説明する。なお、図 6 2 において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

図 6 2 は前記図 3 9 と略々同様な手順を表しており、手順 R 3 2 2 ( 図 3 9 の手順 R 2 0 2 に対応 ) として、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 5 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。当該第 8 の実施の形態の場合、光ディスク記録再生装置 1 0 0 は、不揮発性メモリ 1 1 0 にリボケーションリスト及びレジストレーションリストを格納しているため、当該リストのバージョンナン

バーをセキュリティモジュール 53 に送り、また、セキュリティモジュール 53 は、光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストのバージョンナンバーを、鍵メモリ 36 から読み出して光ディスク記録再生装置 100 に送ることになる。

ここで、上記手順 R 3 2 2 におけるリストのバージョンナンバーの交換により、セキュリティモジュール 53 が保存しているバージョンナンバーの方が、光ディスク記録再生装置 100 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 100 は、手順 R 1 2 3 として、光ディスク情報記録媒体 50 の光ディスク 12 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストを読み出す。

当該光ディスク記録再生装置 100 は、読み出したリストを用いて、当該光ディスク情報記録媒体 50 が正当なものであるか否か検証し、その検証の結果、当該光ディスク情報記録媒体 50 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 50 が正当であると判定した場合、手順 R 3 2 4 として、光ディスク記録再生装置 100 は、上記光ディスク 12 から読み出したリストをセキュリティモジュール 53 に送ると共にその読み出したリストで自身の不揮発性メモリ 110 内のリストを更新する。このときのセキュリティモジュール 53 は、当該リストを用いて、光ディスク記録再生装置 100 が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

上記セキュリティモジュール 53 が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置

100とセキュリティモジュール53の両者が共に正当であると判定した場合は、後段のデータ暗号化と記録の手順R5に進むことになる。

一方、上記手順R322におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置100が保持するリストのバージョンナンバーが、セキュリティモジュール53が保持するバージョンナンバーより新しいか又は同じである場合、光ディスク記録再生装置100は、手順R325として、自己が不揮発性メモリ110に保持するリストをセキュリティモジュール53に送る。

このときのセキュリティモジュール53は、当該リストを用いて、上記光ディスク記録再生装置100が正当であるか否かの検証を行い、不正である場合はプロトコルを終了する。

ここで、上記セキュリティモジュール53が上記リストを用いた検証により正当であると判定した場合、すなわち、光ディスク記録再生装置100が正当であると判定した場合で、且つ、光ディスク記録再生装置100が保持するリストのバージョンナンバーがセキュリティモジュール53が保持するバージョンナンバーと同一である場合は、後段のデータ暗号化と記録の手順R5に進むことになる。

また、上記手順R322におけるリストのバージョンナンバーの交換により、光ディスク記録再生装置100が保持するリストのバージョンナンバーが、セキュリティモジュール53が保持するバージョンナンバーより新しい場合、光ディスク記録再生装置100は、手順R326として、自己が不揮発性メモリ110に保持するリストを、光ディスク12のデータ記録領域に記録する。この際、セキュリティモジュール53は、そのバージョンナンバーを覚え、以後、

使用する。その後、データ暗号化と記録の手順R 5に進むことになる。

<第8の実施の形態の記録処理手順（詳細）>

次に、図6 3には、上記図6 2に示した第8の実施の形態の光ディスク記録再生装置1 0 0が光ディスク情報記録媒体5 0にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図4 1の手順と異なる部分のみ説明する。

この図6 3において、セキュリティモジュール5 3は、手順R 3 3 2（図4 1の手順R 2 2 2に対応）として、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、鍵メモリ3 6に格納されているリストのバージョンナンバー $RevV_A$ 、 $RegV_A$ からなるビット列にパブリック鍵証明書 $Cert_A$ を付け、光ディスク記録再生装置1 0 0に送る。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取った光ディスク記録再生装置1 0 0は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール5 3から返送されてきた乱数 $R_B$ と先に生成したもののが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順R 3 3 3（図4 1の手順R 2 2 3）として、乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、自己の不揮発性メモリ1 1 0に格納しているリストのバージョンナンバー $RevV_B$ 、 $RegV_B$ からなるビット列にデジタル署名を行い、これら $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$ にパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール5 3に送る。

上記光ディスク記録再生装置1 0 0から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$ を受け取ると、セキュリティモジュール5

3は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール53にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置100とセキュリティモジュール53の両方で検証をパスしたとき、セキュリティモジュール53と光ディスク記録再生装置100はセッション鍵 $K_{se}$ を生成して共有する。また、セキュリティモジュール53と光ディスク記録再生装置100は、それぞれリストのバージョンナンバーの新旧の検証を行う。

上記リストのバージョンナンバーの新旧検証により、セキュリティモジュール53が保持するバージョンナンバーの方が、光ディスク記録再生装置100のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置100は、手順R334として、光ディスク情報記録媒体50の光ディスク12のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストを読み出し、そのリストのバージョンナンバーが、先に取得したバージョンナンバー( $RevV_A$ ,  $RegV_A$ )と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体50が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCのデジタル署名 $TC_{Sig}$ の検証を行う。当該検証において、光ディスク情報記録媒体50が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置300は、手順R335として、そのリストをセキュリティモジュール53に送ると共に、当該光ディスク12から読み取ったリストで自己の不揮発性メモリ110内の

リストを更新する。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーがセキュリティモジュールの鍵メモリ 36 内に保持されている前記バージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 100 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、光ディスク記録再生装置 100 が不正なものであると判定した場合は当該プロトコルを終了する。

この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 100 とセキュリティモジュール 53 の両方において正当であると判定した場合は、後段の手順 R 26 以降のデータ暗号化及び記録の処理に進むことになる。

一方、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置 100 のリストのバージョンナンバーの方が、セキュリティモジュール 53 が保持するバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置 100 は、自己が保持するリストを用いて、光ディスク情報記録媒体 50 が正当か否か検証し、その検証でパスしたとき、手順 R 336 として、当該リストをセキュリティモジュール 53 に送る。なお、セキュリティモジュール 53 にリストを送るのは、検証の途中であっても良い。

当該リストを受け取ったセキュリティモジュール 53 は、そのリストのバージョンナンバーが前記バージョンナンバー ( $RevV_B$ ,  $RegV_B$ ) と等しいこと、及び、当該リストを用いて光ディスク記録再



生装置 1 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、光ディスク記録再生装置 1 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。

ここで、上記検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 5 3 の両方において正当であると判定した場合で、且つ光ディスク記録再生装置 1 0 0 が保持するリストのバージョンナンバーがセキュリティモジュール 5 3 が保持するバージョンナンバーと同一である場合は、後段の手順 R 2 6 以降のデータ暗号化及び記録の処理に進むことになる。

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置 1 0 0 が保持するリストのバージョンナンバーが、セキュリティモジュール 5 3 が保持するバージョンナンバーより新しい場合、光ディスク記録再生装置 1 0 0 は、手順 R 3 3 7 として、自己が不揮発性メモリ 1 1 0 に保持するリストを、光ディスク 1 2 のデータ記録領域に記録する。この際、セキュリティモジュール 5 3 は、記憶しているバージョンナンバーを更新する。その後は、手順 R 2 6 以降のデータ暗号化及び記録の処理に進むことになる。

#### < 第 8 の実施例の再生処理手順 >

次に、図 6 4 には、上記第 8 の実施の形態の光ディスク記録再生装置 1 0 0 が光ディスク情報記録媒体 5 0 の光ディスク 1 2 からデータを再生する手順を説明する。なお、図 6 4 の手順は、前記図 4 4 と略々同様であり、以下の説明では、前記図 4 4 とは異なる部分

のみ説明する。

この図 6 4 において、セキュリティモジュール 5 3 は、手順 P 3 3 2 (図 4 4 の手順 P 2 2 2 に対応) として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、鍵メモリ 3 6 に格納されているリストのバージョンナンバー  $RevV_A$ 、 $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 1 0 0 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取った光ディスク記録再生装置 1 0 0 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 5 3 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 P 3 3 3 (図 4 4 の手順 P 2 2 3 に対応) として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己の不揮発性メモリ 1 1 0 に格納しているリストのバージョンナンバー  $RevV_B$ 、 $RegV_B$  からなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 5 3 に送る。

上記光ディスク記録再生装置 1 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 5 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 5 3 にて当該検証をパスしたとき、すなわち、光ディスク記録再生装置 1 0 0 とセキュリティモジュール 5 3 の両方で検証をパスしたとき、セキュリティモジュール 5 3 と光ディスク記録再生装置 1 0 0 はセッション鍵  $K_{se}$  を生成し

て共有する。また、セキュリティモジュール 5 3 と光ディスク記録再生装置 1 0 0 は、それぞれリストのバージョンナンバーの新旧の検証を行う。

上記リストのバージョンナンバーの新旧検証により、セキュリティモジュール 5 3 が保持するバージョンナンバーの方が、光ディスク記録再生装置 1 0 0 のリストのバージョンナンバーより新しい場合、光ディスク記録再生装置 1 0 0 は、手順 P 3 3 4 として、光ディスク情報記録媒体 5 0 の光ディスク 1 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストを読み出し、そのリストのバージョンナンバーが、先に取得したバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 5 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、光ディスク情報記録媒体 5 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、光ディスク記録再生装置 3 0 0 は、手順 P 3 3 5 として、そのリストをセキュリティモジュール 5 3 に送ると共に、当該光ディスク 1 2 から読み取ったリストで自己の不揮発性メモリ 1 1 0 内のリストを更新する。なお、セキュリティモジュール 5 3 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったセキュリティモジュール 5 3 は、そのリストのバージョンナンバーが前記バージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いて光ディスク記録再生装置 1 0 0 が正当なものであるか否かの検証、当該リスト内に含

まれるセンタTCのデジタル署名TCSigの検証を行う。当該検証において、光ディスク記録再生装置100が不正なものであると判定した場合は当該プロトコルを終了する。

この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置100とセキュリティモジュール53の両方において正当であると判定した場合は、後段の手順P26以降のデータ再生及び復号の処理に進むことになる。

一方、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置100のリストのバージョンナンバーの方が、セキュリティモジュール53が保持するバージョンナンバーより新しいか同一の場合、光ディスク記録再生装置100は、自己が保持するリストを用いて、光ディスク情報記録媒体50が正当か否か検証し、その検証でパスしたとき、手順P136として、当該リストをセキュリティモジュール53に送る。なお、セキュリティモジュール53にリストを送るのは、検証の途中であっても良い。

当該リストを受け取ったセキュリティモジュール53は、そのリストのバージョンナンバーが前記バージョンナンバー（RevV<sub>B</sub>, RegV<sub>B</sub>）と等しいこと、及び、当該リストを用いて光ディスク記録再生装置100が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCのデジタル署名TCSigの検証を行う。当該検証において、光ディスク記録再生装置100が不正なものであると判定した場合は当該プロトコルを終了する。

ここで、上記検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置100とセキュリティモジュール53の両方において正当であると判定した場合で、且つ、光ディス

ク記録再生装置 1 0 0 が保持するリストのバージョンナンバーがセキュリティモジュール 5 3 の保持するバージョンナンバーと同一である場合は、後段の手順 P 2 6 以降のデータ再生及び復号の処理に進むことになる。

また、上記リストのバージョンナンバーの新旧検証により、光ディスク記録再生装置 1 0 0 が保持するリストのバージョンナンバーが、セキュリティモジュール 5 3 が保持するバージョンナンバーより新しい場合、光ディスク記録再生装置 1 0 0 は、手順 P 3 3 7 として、自己が不揮発性メモリ 1 1 0 に保持するリストを、光ディスク 1 2 のデータ記録領域に記録する。この際、セキュリティモジュール 5 3 はバージョンナンバーを更新する。その後は、手順 P 2 6 以降のデータ再生及び復号の処理に進むことになる。

〔第 9 の実施の形態 ( I M 2 , D e v 1 ) 〕

次に、第 9 の実施の形態として、メディアタイプ I M 2 とデバイスタイプ D e v 1 の組み合わせ ( I M 2 , D e v 1 ) について説明する。

当該第 9 の実施の形態の組み合わせにおけるシステム構成は、図 6 5 に示すようになる。すなわち、デバイスタイプ D e v 1 の光ディスク記録再生装置 3 0 0 はリストを格納するための専用の前記不揮発性メモリを備えておらず（但し、前述同様に鍵などを格納する鍵メモリ 1 1 1 は備えている）、メディアタイプ I M 2 の光ディスク情報記録媒体 1 0 のセキュリティモジュール 1 3 はリストを格納するための不揮発性メモリ 3 4 を備えている。なお、当該図 6 5 における各部の構成は、前述の図 3 及び図 6 5 の例と同じであるため、それらの説明は省略する。

<第9の実施の形態の記録処理手順>

図66には、当該第9の実施の形態のメディアタイプIM2とデバイスタイプDev1の組み合わせ(IM2, Dev1)の場合に、光ディスク記録再生装置300が光ディスク情報記録媒体10にデータを記録する手順を説明する。なお、図66において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

図66は前記図39と略々同様な手順を表しており、手順R342(図39の手順R202に対応)として、光ディスク記録再生装置300とセキュリティモジュール13との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。当該第9の実施の形態の場合、光ディスク記録再生装置300は、リボケーションリスト及びレジストレーションリストを持たないため、当該手順R342として、リストのバージョンナンバー「0」をセキュリティモジュール13に送り、光ディスク情報記録媒体10は、セキュリティモジュール13内の不揮発性メモリ34に格納されているリストのバージョンナンバーを光ディスク記録再生装置300に送ることになる。

ここで、上記手順R342におけるリストのバージョンナンバーの交換の際、光ディスク記録再生装置300にはリストが存在しないため、セキュリティモジュール13は、不揮発性メモリ34に格納しているリストを用いて光ディスク記録再生装置300が正当なものであるか否か検証し、その検証の結果、当該光ディスク記録再生装置300が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク記録再生装置300が正当であ

ると判定した場合、セキュリティモジュール 13 は、手順 R 343 として、上記不揮発性メモリ 34 に格納しているリボケーションリスト及びレジストレーションリストを光ディスク記録再生装置 300 に送る。

当該光ディスク記録再生装置 300 は、受け取ったリストを用いて、当該光ディスク情報記録媒体 10 が正当なものであるか否か検証し、その検証の結果、当該光ディスク情報記録媒体 10 が不正なものであると判定した時は、当該プロトコルを終了する。一方、その光ディスク情報記録媒体 10 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 5 に進むことになる。

#### < 第 9 の実施の形態の記録処理手順（詳細） >

次に、図 67 には、上記図 66 に示した第 9 の実施の形態の光ディスク記録再生装置 300 が光ディスク情報記録媒体 10 にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図 43 の手順と異なる部分のみ説明する。

この図 67 において、セキュリティモジュール 13 は、手順 R 352（図 43 の手順 R 212 に対応）として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、不揮発性メモリ 34 から読み出したリボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、光ディスク記録再生装置 300 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取った光ディスク記録再生装置 300 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 13 から返送されてきた乱数  $R_B$  と先に生成

したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 3 5 3（図 4 3 の手順 R 2 1 3 に対応）として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 1 3 に送る。

上記光ディスク記録再生装置 3 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  を受け取ると、セキュリティモジュール 1 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。また、セキュリティモジュール 1 3 は、自己が保持するリストを用いて、光ディスク記録再生装置 3 0 0 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 1 3 にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 1 3 の両方で上記検証をパスしたとき、セキュリティモジュール 1 3 と光ディスク記録再生装置 3 0 0 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 1 3 は、手順 R 3 5 4 として、不揮発性メモリ 3 4 に格納しているリストを光ディスク記録再生装置 3 0 0 に送る。

上記リストを受け取った光ディスク記録再生装置 3 0 0 は、そのリストのバージョンナンバーがセキュリティモジュール 1 3 から手順 R 3 5 2 で受け取ったバージョンナンバー（ $RevV_A$ 、 $RegV_A$ ）と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 1 0 が正当なものであるか否かの検証、当該リスト内に含まれるセ



ンタTCのデジタル署名TCSigの検証を行う。当該検証において、光ディスク情報記録媒体10が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置300とセキュリティモジュール13の両方において正当であると判定した場合は、後段の手順R16以降のデータ暗号化及び記録の処理に進むことになる。

#### <第9の実施の形態の再生処理手順>

次に、図68には、上記第9の実施の形態の光ディスク記録再生装置300が光ディスク情報記録媒体10の光ディスク12からデータを再生する手順を説明する。なお、図68の手順は、前記図60と略々同様であり、以下の説明では、前記図60とは異なる部分のみ説明する。

この図68において、セキュリティモジュール13は、手順P352（図60の手順P312に対応）として、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、不揮発性メモリ34から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にパブリック鍵証明書 $Cert_A$ を付け、光ディスク記録再生装置300に送る。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取った光ディスク記録再生装置300は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール13から返送されてきた乱数 $R_B$ と先に生成したものが等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順P353として、乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、リスト

を持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ ,  $R_A$ ,  $V_B$ , 0, 0,  $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 13 に送る。

上記光ディスク記録再生装置 300 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ , 0, 0,  $Sig_B$  を受け取ると、セキュリティモジュール 13 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。また、セキュリティモジュール 13 は、自己が保持するリストを用いて、光ディスク記録再生装置 300 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 13 にて上記検証をパスしたとき、すなわち、光ディスク記録再生装置 300 とセキュリティモジュール 13 の両方で上記検証をパスしたとき、セキュリティモジュール 13 と光ディスク記録再生装置 300 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 13 は、手順 P 354 として、不揮発性メモリ 34 に格納しているリストを光ディスク記録再生装置 300 に送る。

上記リストを受け取った光ディスク記録再生装置 300 は、そのリストのバージョンナンバーがセキュリティモジュール 13 から手順 P 352 で受け取ったバージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いて光ディスク情報記録媒体 10 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名  $TC\ Sig$  の検証を行う。当該検証において、光ディスク情報記録媒体 10 が不正なものであると判定した場合は

当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、光ディスク記録再生装置 3 0 0 とセキュリティモジュール 1 3 の両方において正当であると判定した場合は、後段の手順 P 1 6 以降のデータ再生及び復号の処理に進むことになる。

〔第 1 0 の実施の形態 ( I M 3 , D e v 3 ) 〕

次に、第 1 0 の実施の形態として、メディアタイプ I M 3 とデバイスタイプ D e v 3 の組み合わせ ( I M 3 , D e v 3 ) について説明する。

当該第 1 0 の実施の形態の組み合わせにおけるシステム構成は、図 6 9 に示すようになる。すなわち、デバイスタイプ D e v 3 のメモリ記録再生装置 4 0 0 はリストを格納するための専用の不揮発性メモリを備えておらず（ただし、前述同様に鍵などを格納する鍵メモリ 2 1 1 は備えている）、また、メディアタイプ I M 3 のメモリ情報記録媒体 6 0 のセキュリティモジュール 6 3 はリストを格納するための不揮発性メモリを備えていない（但し、鍵などを格納する鍵メモリ 4 7 は備えている）。なお、当該図 6 9 における各部の構成は、前述の図 1 4 及び図 5 5 の例と同じであるため、それらの説明は省略する。

< 第 1 0 の実施の形態の記録処理手順 >

図 7 0 には、当該第 1 0 の実施の形態のメディアタイプ I M 3 とデバイスタイプ D e v 3 の組み合わせ ( I M 3 , D e v 3 ) の場合に、メモリ記録再生装置 4 0 0 がメモリ情報記録媒体 6 0 にデータを記録する手順を説明する。なお、図 7 0 において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、そ

れらと異なる部分のみ説明する。

図 70 は前記図 45 と略々同様な手順を表しており、手順 R 3 6 2 (図 45 の手順 R 2 3 2 に対応) として、メモリ記録再生装置 4 0 0 とセキュリティモジュール 6 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。ここで、当該第 10 の実施の形態の場合、メモリ記録再生装置 4 0 0 はリストを持たないため、手順 R 3 6 2 として、バージョンナンバー「0」をセキュリティモジュール 6 3 に送り、また、セキュリティモジュール 6 3 は、メモリ部 2 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストのバージョンナンバーを、鍵メモリ 4 7 から読み出してメモリ記録再生装置 4 0 0 に送ることになる。

次に、セキュリティモジュール 6 3 は、手順 R 3 6 3 として、メモリ情報記録媒体 6 0 のメモリ部 2 2 のコンテンツデータ記録用の領域に記録されているリボケーションリスト及びレジストレーションリストを読み出す。セキュリティモジュール 6 3 は、このリストを用いて、メモリ記録再生装置 4 0 0 が正当なものであるか否かの検証を行う。その検証の結果、当該メモリ記録再生装置 4 0 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置 4 0 0 が正当であると判定した場合は、手順 R 3 6 4 として、上記リストをメモリ記録再生装置 4 0 0 に送る。

当該メモリ記録再生装置 4 0 0 は、上記セキュリティモジュール 6 3 から送られたリストを用いて、当該メモリ情報記録媒体 6 0 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報

記録媒体 60 が不正なものであると判定した時は、当該プロトコルを終了する。

一方、上記検証において上記メモリ情報記録媒体 60 が正当であると判定した場合は、すなわち、メモリ記録再生装置 400 とメモリ情報記録媒体 60 の両者が共に正当であると判定された場合は、後段のデータ暗号化と記録の手順 R 35 に進むことになる。

< 第 10 の実施の形態の記録処理手順（詳細） >

次に、図 71 には、上記図 70 に示した第 10 の実施の形態のメモリ記録再生装置 400 がメモリ情報記録媒体 60 にデータを記録するまでの手順の詳細を示しており、前記図 46 と略々同様な手順となっている。

この図 71 において、セキュリティモジュール 63 は、手順 R 372（図 46 の手順 R 242 に対応）として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、鍵メモリ 47 から読み出したリストのバージョンナンバー  $RevV_A$ 、 $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 400 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取ったメモリ記録再生装置 400 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 63 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 373（図 46 の手順 R 243 に対応）として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付

け、セキュリティモジュール 6 3 に送る。

上記メモリ記録再生装置 4 0 0 から  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ , 0, 0,  $Sig_B$  を受け取ると、セキュリティモジュール 6 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 6 3 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 4 0 0 とセキュリティモジュール 6 3 の両方で検証をパスしたとき、セキュリティモジュール 6 3 とメモリ記録再生装置 4 0 0 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 6 3 は、手順 R 3 7 4 として、メモリ部 2 2 のデータ記録領域に格納されているリボケーションリスト及びレジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 4 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名  $TCSig$  の検証を行う。当該検証において、メモリ記録再生装置 4 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール 6 3 は、手順 R 3 7 5 として、そのリストをメモリ記録再生装置 4 0 0 に送る。なお、メモリ記録再生装置 4 0 0 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったメモリ記録再生装置 4 0 0 は、そのリストのバージョンナンバーが先に取得したバージョンナンバー ( $Rev$

$V_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 60 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名  $TC\text{Sig}$  の検証を行う。当該検証において、メモリ情報記録媒体 60 が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置 400 とメモリ情報記録媒体 60 の両方において正当であると判定した場合は、後段の手順 R 46 以降のデータ暗号化及び記録の処理に進むことになる。

#### <第 10 の実施の形態の再生処理手順>

次に、図 72 には、上記第 10 の実施の形態のメモリ記録再生装置 400 がメモリ情報記録媒体 60 のメモリ部 22 からデータを再生する手順を説明する。なお、図 72 の手順は、前記図 50 と略々同様な図面であり、各手順についても略々同じであるため、以下の説明では、前記図 50 とは異なる部分のみ説明する。

この図 72 において、セキュリティモジュール 63 は、手順 P 372 (図 50 の手順 P 242 に対応) として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、鍵メモリ 47 から読み出したリストのバージョンナンバー  $RevV_A$ ,  $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 400 に送る。

これら  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  を受け取ったメモリ記録再生装置 400 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 63 から返送されてきた乱数  $R_B$  と先に生成したものとが等しく、且つデジタル署名  $Sig_A$  が正当であると判定された

とき、手順 P 3 7 3（図 5 0 の手順 P 2 4 3 に対応）として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己がリストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 6 3 に送る。

上記メモリ記録再生装置 4 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  を受け取ると、セキュリティモジュール 6 3 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 6 3 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 4 0 0 とセキュリティモジュール 6 3 の両方で検証をパスしたとき、セキュリティモジュール 6 3 とメモリ記録再生装置 4 0 0 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 6 3 は、手順 P 3 7 4 として、メモリ部 2 2 のデータ記録領域に格納されているリボケーションリスト及びレジストレーションリストを読み取り、そのリストのバージョンナンバーが先に取得したバージョンナンバー（ $RevV_A$ 、 $RegV_A$ ）と等しいこと、及び、当該リストを用いてメモリ記録再生装置 4 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C  $Sig$  の検証を行う。当該検証において、メモリ記録再生装置 4 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、この検証において正当なものであると判定した場合、セキュリティモジュール 6 3 は、手順 P 3 7 5 として、そのリストをメモリ記録再生装置 4 0 0 に送る。なお、メ



メモリ記録再生装置 400 にリストを送るのは、検証の途中であっても良い。

上記リストを受け取ったメモリ記録再生装置 400 は、そのリストのバージョンナンバーがセキュリティーモジュール 63 の鍵メモリ 47 から手順 R 372 によって受けたバージョンナンバー (Rev V<sub>A</sub>, Reg V<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 60 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、メモリ情報記録媒体 60 が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置 400 とセキュリティーモジュール 63 の両方において正当であると判定した場合は、後段の手順 P 46 以降のデータ再生及び復号処理等に進むことになる。

〔第 11 の実施の形態 (IM3, Dev4)〕

次に、第 11 の実施の形態として、メディアタイプ IM3 とデバイスタイプ Dev4 の組み合わせ (IM3, Dev4) について説明する。

当該第 11 の実施の形態の組み合わせにおけるシステム構成は、図 73 に示すようになる。すなわち、デバイスタイプ Dev4 のメモリ記録再生装置 200 はリストを格納するための専用の前記不揮発性メモリ 210 を備えており、一方、メディアタイプ IM3 のメモリ情報記録媒体 60 のセキュリティーモジュール 63 はリストを格納するための不揮発性メモリを備えていない (但し、前述同様に嗅ぎなどを格納する鍵メモリ 47 は備えている)。なお、当該図 73

における各部の構成は、前述の図 1 4 及び図 5 5 の例と同じであるため、それらの説明は省略する。

<第 1 1 の実施の形態の記録処理手順>

図 7 4 には、当該第 1 1 の実施の形態のメディアタイプ I M 3 とデバイスタイプ D e v 4 の組み合わせ ( I M 3 , D e v 4 ) の場合に、メモリ記録再生装置 2 0 0 がメモリ情報記録媒体 6 0 にデータを記録する手順を説明する。なお、図 7 4 において前述の各実施の形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

図 7 4 は前記図 4 5 と略々同様な手順を表しており、手順 R 3 8 2 (図 4 5 の手順 R 2 3 2 に対応) として、メモリ記録再生装置 2 0 0 とセキュリティモジュール 6 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。当該第 1 1 の実施の形態の場合、メモリ記録再生装置 2 0 0 は、不揮発性メモリ 2 1 0 にリボケーションリスト及びレジストレーションリストを格納しているため、当該リストのバージョンナンバーをセキュリティモジュール 6 3 に送り、また、セキュリティモジュール 6 3 は、鍵メモリ 4 7 に格納されているバージョンナンバーをメモリ記録再生装置 2 0 0 に送ることになる。

ここで、上記手順 R 3 8 2 におけるリストのバージョンナンバーの交換により、セキュリティモジュール 6 3 が保持するバージョンナンバーが、メモリ記録再生装置 2 0 0 が保持するリストのバージョンナンバーより新しいか又は同じである場合、セキュリティモジュール 6 3 は、手順 R 3 8 3 として、メモリ部 2 2 に記録されているリストを読み出す。当該セキュリティモジュール 6 3 は、当該リ

ストを用いて、上記メモリ記録再生装置 200 が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置 200 が不正なものであると判定した時は、当該プロトコルを終了する。

一方、そのメモリ記録再生装置 200 が正当であると判定した場合は、すなわち、メモリ記録再生装置 200 とセキュリティモジュール 63 の両者が共に正当であると判定した場合で、且つ、メモリ記録再生装置 200 が保持するリストのバージョンナンバーとセキュリティモジュール 63 が保持するバージョンナンバーとが同一である場合は、後段のデータ暗号化と記録の手順 R 35 に進むことになる。

また、セキュリティモジュール 63 が保持するバージョンナンバーが、メモリ記録再生装置 200 が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール 63 は、手順 R 384 として、上記リストをメモリ記録再生装置 200 に送る。

次に、当該メモリ記録再生装置 200 は、上記供給されたリストを用いて、当該メモリ情報記録媒体 60 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体 60 が不正なものであると判定した時は、当該プロトコルを終了する。

一方、そのメモリ情報記録媒体 60 が正当であると判定した場合は、自己が保持するリストを手順 R 384 で送られたものを用いて更新し、後段のデータ暗号化と記録の手順 R 35 に進むことになる。

また、上記手順 R 382 におけるリストのバージョンナンバーの交換により、メモリ記録再生装置 200 が保持するリストのバージョンナンバーが、セキュリティモジュール 63 が保持するバージョンナンバーより新しい場合、メモリ記録再生装置 200 は、手順 R

385として、自己が保持するリストをセキュリティモジュール63に送る。

セキュリティモジュール63は、当該リストを用いて、上記メモリ記録再生装置200が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置200が不正なものであると判定した時は、当該プロトコルを終了する。

一方、そのメモリ記録再生装置200が正当であると判定した場合は、セキュリティモジュール63は、自己が保持するバージョンナンバーを上記手順R382にて得たバージョンナンバーへ更新すると共に、手順R386として、上記メモリ記録再生装置200から供給されたリストをメモリ部22のデータ記録領域に記録させ、その後、手順R35に進む。

#### <第11の実施の形態の記録処理手順（詳細）>

次に、図75には、上記図74に示した第11の実施の形態のメモリ記録再生装置200がメモリ情報記録媒体60にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図47の手順と異なる部分のみ説明する。

この図75において、セキュリティモジュール63は、手順R392（図47の手順R252に対応）として、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、鍵メモリ47から読み出したリストのバージョンナンバー $RevV_A$ 、 $RegV_A$ からなるビット列にパブリック鍵証明書 $Cert_A$ を付け、メモリ記録再生装置200に送る。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取ったメモリ記録再生装置200は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキ

セキュリティモジュール 63 から返送されてきた乱数  $R_B$  と先に生成したものとの等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 393 (図 47 の手順 R 253 に対応) として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己の不揮発性メモリ 210 に格納しているリストのバージョンナンバー  $RevV_B$ 、 $RegV_B$  からなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 63 に送る。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 63 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 63 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 200 とセキュリティモジュール 63 の両方で検証をパスしたとき、セキュリティモジュール 63 とメモリ記録再生装置 200 はセッション鍵  $K_{se}$  を生成して共有する。

また、セキュリティモジュール 63 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 63 とメモリ記録再生装置 200 は、それぞれリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール 63 は、手順 R 394 として、メモリ部 22 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー ( $RevV_A$ 、 $RegV_A$ ) と等しいこと、及び、当

該リストを用いてメモリ記録再生装置 200 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 200 が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置 200 は、自己が保持するリストを用いて、メモリ情報記録媒体 60 が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール 63 及びメモリ記録再生装置 200 において、共に正当であると判定した時は、その後の手順 R 56 以降に進むことになる。

また、両者のバージョンナンバーの検証を行った結果、セキュリティモジュール 63 が保持するリストのバージョンナンバーが、メモリ記録再生装置 200 が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール 63 は、手順 R 395 として、メモリ部 22 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 200 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 200 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置 200 が正当であると判定した場合は、手順 R 396 として、上記リストをメモリ記録再生装置 200 に送る。

メモリ記録再生装置 200 は、当該リストを受け取ると、そのリストのバージョンナンバーが先にセキュリティモジュール 63 から

手順 R 3 9 2 で取得したバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、メモリ情報記録媒体 6 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体 6 0 が正当であると判定した場合は、送られてきたリストを用いて自己のリストを更新し、その後の手順 R 5 6 以降に進むことになる。

また、両者のバージョンナンバーの検証を行った結果、メモリ記録再生装置 2 0 0 が保持するリストのバージョンナンバーが、セキュリティモジュール 6 3 が保持するバージョンナンバーより新しい場合、メモリ記録再生装置 2 0 0 は、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体 6 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体 6 0 が正当であると判定した場合は、手順 R 3 9 7 として、上記リストをセキュリティモジュール 6 3 に送る。

セキュリティモジュール 6 3 は、当該リストを受け取ると、そのリストのバージョンナンバーが先にメモリ記録再生装置 2 0 0 から手順 R 3 9 3 で取得したバージョンナンバー (RevV<sub>B</sub>, RegV<sub>B</sub>) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 2 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ T C のデジタル署名 T C Sig の検証を行う。当該検証において、メモリ記録再生装置 2 0 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置 2 0 0 が正当で

あると判定した場合、セキュリティモジュール 63 は、自己が保持するバージョンナンバーを、手順 R 393 で得られたバージョンナンバーへ更新すると共に、手順 R 398 として、上記リストをメモリ部 22 に書き込んで更新し、その後の手順 R 56 以降に進むことになる。なお、リストの更新と手順 R 56 以降の処理は前後してもかまわない。これらのメディアタイプ IM3 では、鍵メモリ 47 に格納されているリストのバージョンを読み出すようにしているが、例えば、メモリ部 22 からリストのバージョンをプロトコル中で読み出すようにしてもよい。但し、メモリ部 22 上でのリストの改ざんを防止するためには、上述のようにバージョンナンバーをセキュリティモジュール 63（鍵メモリ 47）が記憶しておくことが望ましい。

#### <第 11 の実施の形態の再生処理手順>

次に、図 76 には、上記第 11 の実施の形態のメモリ記録再生装置 200 がメモリ情報記録媒体 60 のメモリ部 22 からデータを再生する手順を説明する。なお、図 76 の手順は、前記図 51 と略々同様であり、以下の説明では、前記図 51 とは異なる部分のみ説明する。

この図 76 において、セキュリティモジュール 63 は、手順 P 392（図 51 の手順 P 252 に対応）として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、鍵メモリ 47 から読み出したリストのバージョンナンバー  $RevV_A$ 、 $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 200 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取ったメモリ記録再生装置 200 は、パブリック鍵証明書  $Cert_A$ 、



デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 63 から返送されてきた乱数  $R_B$  と先に生成したものとの等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 P.393 (図 51 の手順 P.253 に対応) として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、自己の不揮発性メモリ 210 に格納しているリストのバージョンナンバー  $RevV_B$ 、 $RegV_B$  からなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 63 に送る。

上記メモリ記録再生装置 200 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、 $RevV_B$ 、 $RegV_B$ 、 $Sig_B$  を受け取ると、セキュリティモジュール 63 は、パブリック鍵証明書  $Cert_B$ 、デジタル署名  $Sig_B$  の検証を行う。この検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 63 にて当該検証をパスしたとき、すなわち、メモリ記録再生装置 200 とセキュリティモジュール 63 の両方で検証をパスしたとき、セキュリティモジュール 63 とメモリ記録再生装置 200 はセッション鍵  $K_{se}$  を生成して共有する。

また、セキュリティモジュール 63 とメモリ記録再生装置 200 の両者において、共に相手方が正当であると検証された場合、セキュリティモジュール 63 とメモリ記録再生装置 200 は、それぞれリストのバージョンナンバーのチェックを行う。

ここで、両者のバージョンナンバーが同じである場合、セキュリティモジュール 63 は、手順 P.394 として、メモリ部 22 からリストを読み出し、そのリストのバージョンナンバーが先に取得した

バージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 200 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 200 が不正なものであると判定した場合は当該プロトコルを終了する。また、この時のメモリ記録再生装置 200 は、自己が保持するリストを用いて、メモリ情報記録媒体 60 が正当であるか否かの検証を行い、不正なものであると判定したときは当該プロトコルを終了し、これらセキュリティモジュール 63 及びメモリ記録再生装置 200 において、共に正当であると判定した時は、その後の手順 R56 以降に進むことになる。

また、両者のバージョンナンバーの検証を行った結果、セキュリティモジュール 63 が保持するバージョンナンバーが、メモリ記録再生装置 200 が保持するリストのバージョンナンバーより新しい場合、セキュリティモジュール 63 は、手順 P395 として、メモリ部 22 からリストを読み出し、そのリストのバージョンナンバーが先に取得したバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 200 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 200 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ記録再生装置 200 が正当であると判定した場合は、手順 P396 として、上記リストをメモリ記録再生装置 200 に送る。

メモリ記録再生装置 200 は、当該リストを受け取ると、そのリ

ストのバージョンナンバーが先にセキュリティモジュール 6 3 から手順 P 3 9 2 で取得したバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ情報記録媒体 6 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体 6 0 が正当であると判定した場合は、送られたリストを用いて自己のリストを更新し、その後の手順 P 5 6 以降に進むことになる。

また、両者のバージョンナンバーの検証を行った結果、セキュリティモジュール 6 3 が保持するバージョンナンバーが、メモリ情報記録媒体 6 0 のメモリ部 2 2 が保持するリストのバージョンナンバーより新しい場合、メモリ記録再生装置 2 0 0 は、当該リストを用いてメモリ情報記録媒体 6 0 が正当なものであるか否かを検証し、当該検証において、メモリ情報記録媒体 6 0 が不正なものであると判定した場合は当該プロトコルを終了する。一方、メモリ情報記録媒体 6 0 が正当であると判定した場合は、手順 P 3 9 7 として、上記リストをセキュリティモジュール 6 3 に送る。

セキュリティモジュール 6 3 は、当該リストを受け取ると、そのリストのバージョンナンバーが先にメモリ記録再生装置 2 0 0 から手順 P 3 9 3 で取得したバージョンナンバー (RevV<sub>B</sub>, RegV<sub>B</sub>) と等しいこと、及び、当該リストを用いてメモリ記録再生装置 2 0 0 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名 TC Sig の検証を行う。当該検証において、メモリ記録再生装置 2 0 0 が不正なものであると判定した場合は当

該プロトコルを終了する。一方、メモリ記録再生装置 200 が正当であると判定した場合は、セキュリティモジュール 63 は、自己が保持するバージョンナンバーを手順 P 393 で得たバージョンナンバーへ更新すると共に、手順 P 398 として、上記リストをメモリ部 22 に書き込んで更新し、その後の手順 P 56 以降に進むことになる。なお、リストの更新と手順 P 56 以降の処理は前後してもかまわない。

〔第 12 の実施の形態 (IM4, Dev3)〕

次に、第 12 の実施の形態として、メディアタイプ IM4 とデバイスタイプ Dev3 の組み合わせ (IM4, Dev3) について説明する。

当該第 12 の実施の形態の組み合わせにおけるシステム構成は、図 77 に示すようになる。すなわち、デバイスタイプ Dev3 のメモリ記録再生装置 400 はリストを格納するための専用の前記不揮発性メモリを備えておらず（但し、前述同様に鍵などを格納する鍵メモリ 211 は備えている）、一方、メディアタイプ IM4 のメモリ情報記録媒体 20 のセキュリティモジュール 23 はリストを格納するための不揮発性メモリ 43 を備えている。なお、当該図 77 における各部の構成は、前述の図 14 及び図 69) の例と同じであるため、それらの説明は省略する。

<第 12 の実施の形態の記録処理手順>

図 78 には、当該第 12 の実施の形態のメディアタイプ IM4 とデバイスタイプ Dev3 の組み合わせ (IM4, Dev3) の場合に、メモリ記録再生装置 400 がメモリ情報記録媒体 10 にデータを記録する手順を説明する。なお、図 78 において前述の各実施の

形態の略々同じ手順についての説明は省略し、以下の説明では、それらと異なる部分のみ説明する。

図 7 8 は前記図 4 5 と略々同様な手順を表しており、手順 R 4 0 2 (図 4 5 の手順 2 3 2 に対応) として、メモリ記録再生装置 4 0 0 とセキュリティモジュール 2 3 との間でリボケーションリスト及びレジストレーションリストのバージョンナンバーを交換する。当該第 1 2 の実施の形態の場合、メモリ記録再生装置 2 0 0 は、リボケーションリスト及びレジストレーションリストを持たないため、当該リストのバージョンナンバーとして「0」をセキュリティモジュール 2 3 に送り、メモリ情報記録媒体 2 0 は、セキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に格納されているリストのバージョンナンバーをメモリ記録再生装置 4 0 0 に送ることになる。

ここで、上記手順 R 4 0 2 におけるリストのバージョンナンバーの交換により、メモリ記録再生装置 4 0 0 にはリストが存在しないため、セキュリティモジュール 2 3 は、不揮発性メモリ 4 4 に格納しているリストを用いてメモリ記録再生装置 4 0 0 が正当なものであるか否か検証し、その検証の結果、当該メモリ記録再生装置 4 0 0 が不正なものであると判定した時は、当該プロトコルを終了する。一方、そのメモリ記録再生装置 4 0 0 が正当であると判定した場合、セキュリティモジュール 2 3 は、手順 R 4 0 3 として、上記不揮発性メモリ 4 4 に格納しているリボケーションリスト及びレジストレーションリストをメモリ記録再生装置 4 0 0 に送る。

当該メモリ記録再生装置 4 0 0 は、受け取ったリストを用いて、当該メモリ情報記録媒体 2 0 が正当なものであるか否か検証し、その検証の結果、当該メモリ情報記録媒体 2 0 が不正なものであると

判定した時は、当該プロトコルを終了する。一方、そのメモリ情報記録媒体 20 が正当であると判定した場合は、後段のデータ暗号化と記録の手順 R 3 5 に進むことになる。

< 第 1 2 の実施の形態の記録処理手順（詳細） >

次に、図 7 9 には、上記図 7 8 に示した第 1 2 の実施の形態のメモリ記録再生装置 4 0 0 がメモリ情報記録媒体 20 にデータを記録するまでの手順の詳細を示している。なお、以下の説明では、前記図 4 6 の手順と異なる部分のみ説明する。

この図 7 9 において、セキュリティモジュール 2 3 は、手順 R 4 1 2（図 4 6 の手順 R 2 4 2 に対応）として、乱数  $R_A$ 、乱数  $R_B$ 、値  $V_A$ 、不揮発性メモリ 4 4 から読み出したリボケーションリストのバージョンナンバー  $RevV_A$ 、レジストレーションリストのバージョンナンバー  $RegV_A$  からなるビット列にパブリック鍵証明書  $Cert_A$  を付け、メモリ記録再生装置 4 0 0 に送る。

これら  $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$  を受け取ったメモリ記録再生装置 4 0 0 は、パブリック鍵証明書  $Cert_A$ 、デジタル署名  $Sig_A$  の検証を行い、その検証をパスし、さらに、セキュリティモジュール 2 3 から返送されてきた乱数  $R_B$  と先に生成したもののが等しく、且つデジタル署名  $Sig_A$  が正当であると判定されたとき、手順 R 4 1 3（図 4 6 の手順 R 2 4 3 に対応）として、乱数  $R_B$ 、乱数  $R_A$ 、値  $V_B$ 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら  $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$  にパブリック鍵証明書  $Cert_B$  を付け、セキュリティモジュール 2 3 に送る。

上記メモリ記録再生装置 4 0 0 から  $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、0、

0,  $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行う。また、セキュリティモジュール23は、自己が保持するリストを用いて、メモリ記録再生装置400が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール23にて上記検証をパスしたとき、すなわち、メモリ記録再生装置400とセキュリティモジュール23の両方で上記検証をパスしたとき、セキュリティモジュール23とメモリ記録再生装置400はセッション鍵 $K_{se}$ を生成して共有する。

次に、セキュリティモジュール23は、手順R414として、不揮発性メモリ44に格納しているリストをメモリ記録再生装置400に送る。

上記リストを受け取ったメモリ記録再生装置400は、そのリストのバージョンナンバーがセキュリティモジュール23から手順R412で受け取ったバージョンナンバー( $RevV_A$ ,  $RegV_A$ )と等しいこと、及び、当該リストを用いてメモリ情報記録媒体20が正当なものであるか否かの検証、当該リスト内に含まれるセンタTCのデジタル署名 $TC_{Sig}$ の検証を行う。当該検証において、メモリ情報記録媒体20が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置400とセキュリティモジュール23の両方において正当であると判定した場合は、後段の手順R46以降のデータ暗号化及び記録の処理に進むことになる。

<第12の実施の形態の再生処理手順>

次に、図80には、上記第12の実施の形態のメモリ記録再生装置400がメモリ情報記録媒体20のメモリ部22からデータを再生する手順を説明する。なお、図80の手順は、前記図50と略々同様であり、以下の説明では、前記図50とは異なる部分のみ説明する。

この図80において、セキュリティモジュール23は、手順P412（図50の手順P242に対応）として、乱数 $R_A$ 、乱数 $R_B$ 、値 $V_A$ 、不揮発性メモリ44から読み出したリボケーションリストのバージョンナンバー $RevV_A$ 、レジストレーションリストのバージョンナンバー $RegV_A$ からなるビット列にパブリック鍵証明書 $Cert_A$ を付け、メモリ記録再生装置400に送る。

これら $Cert_A$ 、 $R_A$ 、 $R_B$ 、 $V_A$ 、 $RevV_A$ 、 $RegV_A$ 、 $Sig_A$ を受け取ったメモリ記録再生装置400は、パブリック鍵証明書 $Cert_A$ 、デジタル署名 $Sig_A$ の検証を行い、その検証をパスし、さらに、セキュリティモジュール23から返送されてきた乱数 $R_B$ と先に生成したものとの等しく、且つデジタル署名 $Sig_A$ が正当であると判定されたとき、手順P413（図50の手順P243に対応）として、乱数 $R_B$ 、乱数 $R_A$ 、値 $V_B$ 、リストを持たないことを示す「0」のバージョンナンバーからなるビット列にデジタル署名を行い、これら $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$ にパブリック鍵証明書 $Cert_B$ を付け、セキュリティモジュール23に送る。

上記メモリ記録再生装置400から $Cert_B$ 、 $R_B$ 、 $R_A$ 、 $V_B$ 、0、0、 $Sig_B$ を受け取ると、セキュリティモジュール23は、パブリック鍵証明書 $Cert_B$ 、デジタル署名 $Sig_B$ の検証を行う。また、セキュ



リティモジュール 23 は、自己が保持するリストを用いて、メモリ記録再生装置 400 が正当であるか否かの検証を行う。これら検証をパスしなかった場合は、当該プロトコルを終了する。

ここで、セキュリティモジュール 23 にて上記検証をパスしたとき、すなわち、メモリ記録再生装置 400 とセキュリティモジュール 23 の両方で上記検証をパスしたとき、セキュリティモジュール 23 とメモリ記録再生装置 400 はセッション鍵  $K_{se}$  を生成して共有する。

次に、セキュリティモジュール 23 は、手順 P 414 として、不揮発性メモリ 44 に格納しているリストをメモリ記録再生装置 400 に送る。

上記リストを受け取ったメモリ記録再生装置 400 は、そのリストのバージョンナンバーがセキュリティモジュール 23 から手順 P 412 で受け取ったバージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) と等しいこと、及び、当該リストを用いてメモリ情報記録媒体 20 が正当なものであるか否かの検証、当該リスト内に含まれるセンタ TC のデジタル署名  $TC_{Sig}$  の検証を行う。当該検証において、メモリ情報記録媒体 20 が不正なものであると判定した場合は当該プロトコルを終了する。

一方、この検証において正当なものであると判定した場合、すなわち、メモリ記録再生装置 400 とセキュリティモジュール 23 の両方において正当であると判定した場合は、後段の手順 P 16 以降のデータ再生及び復号の処理に進むことになる。

〔メディアタイプ／デバイスタイプ別処理手順〕

次に、図 81 乃至図 87 のフローチャートを用いて、本発明の各

実施の形態のセキュリティモジュールと記録再生装置が、それぞれタイプ別に行う処理の流れを説明する。なお、以下の説明では、リボケーションリスト及びレジストレーションリストの両方を用いた場合を例に挙げている。

〔メディアタイプ別処理手順〕

<メディアタイプIM1>

図81には、前記メディアタイプIM1に相当する光ディスク情報記録媒体50のセキュリティモジュール53における処理の流れを示す。

この図81において、セキュリティモジュール53は、ステップS1として、前述したように、光ディスク記録再生装置が発生した乱数 $R_B$ の受信と、前記 $V_A = K_A \cdot G$ の計算、乱数 $R_A$ の発生、デジタル署名を行い $Sig_A$ 計算、 $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$ を光ディスク記録再生装置に送信する。

次に、セキュリティモジュール53は、ステップS2として、光ディスク記録再生装置から送信されてきた $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$ 受信、 $Cert_B$ の検証、 $Sig_B$ の検証、セッション鍵 $K_{se}$ の計算を行う。

次に、セキュリティモジュール53は、ステップS3として、例えばリストのバージョンナンバーが「0」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップS3の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプDev1（すなわち前記光ディスク記録再生装置300）であると判定した場合、セキュリティモジュール53の処理は、ステップS4に進む。一方、ステッ

プS 3の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev 2（すなわち前記光ディスク記録再生装置100）であると判定した場合、セキュリティモジュール53の処理は、ステップS 5に進む。

ステップS 4の処理に進むと、セキュリティモジュール53は、光ディスク記録再生装置が光ディスク12のデータ記録領域から読み出して送信したリボケーションリスト及びレジストレーションリストを受信し、そのバージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）の検証と、そのリストを用いた光ディスク記録再生装置（デバイスタイプDev 1の装置300）のID<sub>B</sub>の検証と、センタTCのデジタル署名TCSigの検証を行った後、ステップS 8に進む。

また、ステップS 5の処理に進むと、セキュリティモジュール53は、光ディスク12のデータ記録領域に記録されているリボケーションリスト及びレジストレーションリストのバージョンが、デバイスタイプDev 2の光ディスク記録再生装置100の保持するリストのバージョンナンバーよりも大きい（ $A > B$ ）か、或いはそれ以下（ $A \leq B$ ）であるのかの判定を行う。このステップS 5の判定において、 $A > B$ であると判定した場合、セキュリティモジュール53の処理はステップS 6に進み、一方、 $A \leq B$ であると判定した場合、セキュリティモジュール53の処理はステップS 7に進む。

ステップS 6の処理に進むと、セキュリティモジュール53は、光ディスク記録再生装置が、光ディスク12のデータ記録領域から読み出して送信したリボケーションリスト及びレジストレーションリストを受信し、そのバージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）の検証と、そのリストを用いた光ディスク記録再生装置100のID

Bの検証と、センタTCのデジタル署名TCSigの検証を行った後、ステップS8に進む。

また、ステップS7の処理に進むと、セキュリティモジュール53は、光ディスク記録再生装置100が保持するリボケーションリスト及びレジストレーションリストを受け取り、そのバージョンナンバー(RevV<sub>B</sub>, RegV<sub>B</sub>)の検証と、そのリストを用いた光ディスク記録再生装置100のID<sub>B</sub>の検証と、センタTCのデジタル署名TCSigの検証を行った後、ステップS8に進む。

ステップS8の処理に進むと、セキュリティモジュール53は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

当該ステップS8にて記録の処理が要求されていると判定した場合、セキュリティモジュール53は、ステップS9の処理として、光ディスク記録再生装置がセッション鍵K<sub>se</sub>にて暗号鍵K<sub>co</sub>を暗号化した値Enc(K<sub>se</sub>, K<sub>co</sub>)を受信して復号し、次に、その復号により得られた暗号鍵K<sub>co</sub>を自己が保持するストレージ鍵K<sub>st</sub>で暗号化した値Enc(K<sub>st</sub>, K<sub>co</sub>)を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵K<sub>co</sub>にて暗号化されたコンテンツデータEnc(K<sub>co</sub>, data)と暗号鍵K<sub>co</sub>をストレージ鍵K<sub>st</sub>で暗号化した値Enc(K<sub>st</sub>, K<sub>co</sub>)が、光ディスク12に記録されることになる。

一方、ステップS8にて再生の処理が要求されていると判定した場合、セキュリティモジュール53は、ステップS10の処理として、光ディスク記録再生装置が光ディスク12のデータ記録領域などから読み出して送信したストレージ鍵K<sub>st</sub>にて暗号鍵K<sub>co</sub>が暗号

化されている値  $E_{nc}(K_{st}, K_{co})$  を受信して復号し、その復号により得られた暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  にて暗号化した値  $E_{nc}(K_{se}, K_{co})$  を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵  $K_{co}$  にて暗号化されているコンテンツデータ  $E_{nc}(K_{co}, \text{data})$  は、光ディスク 12 から再生されて光ディスク記録再生装置に送られることになる。

#### <メディアタイプ IM2>

図 8 2 には、前記メディアタイプ IM2 に相当する光ディスク情報記録媒体 10 のセキュリティモジュール 13 における処理の流れを示す。

この図 8 2 において、セキュリティモジュール 13 は、ステップ S 1 1 として、前述したように、光ディスク記録再生装置が発生した乱数  $R_B$  の受信と、前記  $V_A = K_A \cdot G$  の計算、乱数  $R_A$  の発生、デジタル署名を行い  $\text{Sig}_A$  計算、 $\text{Cert}_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $\text{Rev}V_A$ ,  $\text{Reg}V_A$ ,  $\text{Sig}_A$  を光ディスク記録再生装置に送信する。

次に、セキュリティモジュール 13 は、ステップ S 1 2 として、光ディスク記録再生装置から送信されてきた  $\text{Cert}_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $\text{Rev}V_B$ ,  $\text{Reg}V_B$ ,  $\text{Sig}_B$  受信、 $\text{Cert}_B$  の検証、 $\text{Sig}_B$  の検証、セッション鍵  $K_{se}$  の計算を行う。

次に、セキュリティモジュール 13 は、ステップ S 1 3 として、例えばリストのバージョンナンバーが「0」か否かにより、相手方の光ディスク記録再生装置のデバイスタイプを判定する。このステップ S 1 3 の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプ  $\text{Dev}1$  (光ディスク記録再生装置 300) であると判定した場合、セキュリティモジュール

ル 1 3 の処理は、ステップ S 1 4 に進む。一方、ステップ S 1 3 の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプ D e v 2（光ディスク記録再生装置 1 0 0）であると判定した場合、セキュリティモジュール 1 3 の処理は、ステップ S 1 5 に進む。

ステップ S 1 4 の処理に進むと、セキュリティモジュール 1 3 は、不揮発性メモリ 3 4 に格納しているリストを用いて光ディスク記録再生装置 3 0 0 の I D<sub>B</sub>を検証し、その検証をパスしたとき、上記リストを光ディスク記録再生装置 3 0 0 に送信した後、ステップ S 1 9 の処理に進む。

また、ステップ S 1 5 の処理に進むと、セキュリティモジュール 1 3 は、不揮発性メモリ 3 4 に格納しているリストのバージョンが、光ディスク記録再生装置 1 0 0 が保持するリストのバージョンナンバーよりも大きい ( $A > B$ ) か、或いは等しいか ( $A = B$ )、或いは小さいか ( $A < B$ ) の判定を行う。このステップ S 1 5 の判定において、 $A > B$  であると判定した場合、セキュリティモジュール 1 3 の処理はステップ S 1 6 に進み、 $A = B$  であると判定した場合、セキュリティモジュール 1 3 の処理はステップ S 1 7 に進み、 $A > B$  であると判定した場合、セキュリティモジュール 1 3 の処理はステップ S 1 8 に進む。

ステップ S 1 6 の処理に進むと、セキュリティモジュール 1 3 は、自己が保持するリストを用いて光ディスク記録再生装置 1 0 0 の I D<sub>B</sub>の検証を行い、そのリストを光ディスク記録再生装置 1 0 0 に送信した後、ステップ S 1 9 に進む。

また、ステップ S 1 7 の処理に進むと、セキュリティモジュール

13は、自己が保持するリストを用いて光ディスク記録再生装置100のID<sub>B</sub>の検証を行った後、ステップS19に進む。

また、ステップS18の処理に進むと、セキュリティモジュール13は、光ディスク記録再生装置100からリストを受信し、そのバージョンナンバー(RevV<sub>B</sub>, RegV<sub>B</sub>)の検証と、当該リストを用いた光ディスク記録再生装置100のID<sub>B</sub>の検証と、センタTCのデジタル署名TCSigの検証を行った後、検証が成功であれば自己のリストを送られたリストを用いて更新してステップS19に進む。

ステップS19の処理に進むと、セキュリティモジュール13は、光ディスク記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

当該ステップS19にて記録の処理が要求されていると判定した場合、セキュリティモジュール13は、ステップS20の処理として、光ディスク記録再生装置がセッション鍵K<sub>se</sub>にて暗号鍵K<sub>co</sub>を暗号化した値Enc(K<sub>se</sub>, K<sub>co</sub>)を受信して復号し、次に、その復号により得られた暗号鍵K<sub>co</sub>を自己が保持するストレージ鍵K<sub>st</sub>で暗号化した値Enc(K<sub>st</sub>, K<sub>co</sub>)を生成して光ディスク記録再生装置に送信する。その後、光ディスク記録再生装置において上記暗号鍵K<sub>co</sub>にて暗号化されたコンテンツデータEnc(K<sub>co</sub>, data)と暗号鍵K<sub>co</sub>をストレージ鍵K<sub>st</sub>で暗号化した値Enc(K<sub>st</sub>, K<sub>co</sub>)が、光ディスク12に記録されることになる。

一方、ステップS19にて再生の処理が要求されていると判定した場合、セキュリティモジュール13は、ステップS21の処理として、光ディスク記録再生装置が光ディスク12のデータ記録領域などから読み出して送信した、ストレージ鍵K<sub>st</sub>にて暗号鍵K<sub>co</sub>が

暗号化されている値  $E_{nc}(K_{st}, K_{co})$  を受信して復号し、その復号により得られた暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  にて暗号化した値  $E_{nc}(K_{se}, K_{co})$  を生成して光ディスク記録再生装置に送信する。その後、上記暗号鍵  $K_{co}$  にて暗号化されているコンテンツデータ  $E_{nc}(K_{co}, \text{data})$  は、光ディスク 12 から再生されて光ディスク記録再生装置に送られることになる。

#### <メディアタイプ IM3>

図 83 には、前記メディアタイプ IM3 に相当するメモリ情報記録媒体 60 のセキュリティモジュール 63 における処理の流れを示す。

この図 83 において、セキュリティモジュール 63 は、ステップ S31 として、前述したように、メモリ記録再生装置が発生した乱数  $R_B$  の受信と、前記  $V_A = K_A \cdot G$  の計算、乱数  $R_A$  の発生、デジタル署名を行い  $\text{Sig}_A$  計算、 $\text{Cert}_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $\text{Rev}V_A$ ,  $\text{Reg}V_A$ ,  $\text{Sig}_A$  をメモリ記録再生装置に送信する。

次に、セキュリティモジュール 63 は、ステップ S32 として、メモリ記録再生装置から送信されてきた  $\text{Cert}_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $\text{Rev}V_B$ ,  $\text{Reg}V_B$ ,  $\text{Sig}_B$  受信、 $\text{Cert}_B$  の検証、 $\text{Sig}_B$  の検証、セッション鍵  $K_{se}$  の計算を行う。

次に、セキュリティモジュール 63 は、ステップ S33 として、例えばリストのバージョンナンバーが「0」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップ S33 の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプ  $\text{Dev}3$  (メモリ記録再生装置 400) であると判定した場合、セキュリティモジュール 6



3の処理は、ステップS34に進む。一方、ステップS33の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev4（メモリ記録再生装置200）であると判定した場合、セキュリティモジュール63の処理は、ステップS35に進む。

ステップS34の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に格納しているリストを読み出してバージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）の検証と、それを用いてメモリ記録再生装置400のID<sub>B</sub>の検証とセンターTCのデジタル署名TCSigの検証を行い、その検証をパスしたとき、上記リストをメモリ記録再生装置400に送信した後、ステップS39の処理に進む。

また、ステップS35の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に格納しているリストのバージョンが、メモリ記録再生装置200が保持するリストのバージョンナンバーよりも大きい（ $A > B$ ）か、或いは等しいか（ $A = B$ ）、或いは小さいか（ $A < B$ ）の判定を行う。このステップS35の判定において、 $A > B$ であると判定した場合、セキュリティモジュール63の処理はステップS36に進み、 $A = B$ であると判定した場合、セキュリティモジュール63の処理はステップS37に進み、 $A < B$ であると判定した場合、セキュリティモジュール63の処理はステップS38に進む。

ステップS36の処理に進むと、セキュリティモジュール63は、メモリ部22のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー（RevV<sub>A</sub>, RegV<sub>A</sub>）の検証と、当該リス

トを用いたメモリ記録再生装置 200 の  $ID_B$  の検証と、センタ TC のデジタル署名 TC Sig の検証を行い、さらに当該リストをメモリ記録再生装置 200 に送信した後、ステップ S 39 に進む。

また、ステップ S 37 の処理に進むと、セキュリティモジュール 63 は、メモリ部 22 のデータ記録領域に記録されていたリストを読み出し、そのバージョンナンバー ( $RevV_A$ ,  $RegV_A$ ) の検証と、当該リストを用いたメモリ記録再生装置 200 の  $ID_B$  の検証と、センタ TC のデジタル署名 TC Sig の検証を行った後、ステップ S 39 に進む。

また、ステップ S 38 の処理に進むと、セキュリティモジュール 63 は、メモリ記録再生装置 200 からリストを受信し、そのバージョンナンバー ( $RevV_B$ ,  $RegV_B$ ) の検証と、当該リストを用いたメモリ記録再生装置 200 の  $ID_B$  の検証と、センタ TC のデジタル署名 TC Sig の検証を行い、さらに、そのリストをメモリ部 22 に書き込んで更新した後、ステップ S 39 に進む。

ステップ S 39 の処理に進むと、セキュリティモジュール 63 は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

当該ステップ S 39 にて記録の処理が要求されていると判定した場合、セキュリティモジュール 63 は、ステップ S 40 の処理として、メモリ記録再生装置がセッション鍵  $K_{se}$  にて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{se}, K_{co})$  を受信して復号し、次に、その復号により得られた暗号鍵  $K_{co}$  を自己が保持するストレージ鍵  $K_{st}$  で暗号化した値  $E_{nc}(K_{st}, K_{co})$  を生成してメモリ部 22 に書き込む。その後、セキュリティモジュール 63 は、上記メモリ記録再生装置にお

いて上記暗号鍵  $K_{co}$  にて暗号化されたコンテンツデータ  $E_{nc}(K_{co}, data)$  を受信し、メモリ部 22 に記録する。

一方、ステップ S 39 にて再生の処理が要求されていると判定した場合、セキュリティモジュール 63 は、ステップ S 41 の処理として、ストレージ鍵  $K_{st}$  にて暗号鍵  $K_{co}$  が暗号化され例えばメモリ部 22 のデータ記録領域等に記録されている値  $E_{nc}(K_{st}, K_{co})$  を読み出して復号し、その復号により得られた暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  にて暗号化した値  $E_{nc}(K_{se}, K_{co})$  を生成してメモリ記録再生装置に送信する。その後、セキュリティモジュール 63 は、メモリ部 22 から上記暗号鍵  $K_{co}$  にて暗号化されているコンテンツデータ  $E_{nc}(K_{co}, data)$  を読み出し、メモリ記録再生装置に送る。

#### <メディアタイプ IM4>

図 84 には、前記メディアタイプ IM4 に相当するメモリ情報記録媒体 20 のセキュリティモジュール 23 における処理の流れを示す。

この図 84 において、セキュリティモジュール 23 は、ステップ S 51 として、前述したように、メモリ記録再生装置が発生した乱数  $R_B$  の受信と、前記  $V_A = K_A \cdot G$  の計算、乱数  $R_A$  の発生、デジタル署名を行い  $Sig_A$  計算、 $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  をメモリ記録再生装置に送信する。

次に、セキュリティモジュール 23 は、ステップ S 52 として、メモリ記録再生装置から送信されてきた  $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  受信、 $Cert_B$  の検証、 $Sig_B$  の検証、セッション鍵  $K_{se}$  の計算を行う。

次に、セキュリティモジュール 23 は、ステップ S 53 として、

例えばリストのバージョンナンバーが「0」か否かにより、相手方のメモリ記録再生装置のデバイスタイプを判定する。このステップS 5 3の判定において、例えばリストのバージョンナンバーが「0」となっており、前記デバイスタイプDev 3（メモリ記録再生装置4 0 0）であると判定した場合、セキュリティモジュール2 3の処理は、ステップS 5 4に進む。一方、ステップS 5 3の判定において、リストのバージョンナンバーが「0」でなく、前記デバイスタイプDev 4（メモリ記録再生装置2 0 0）であると判定した場合、セキュリティモジュール2 3の処理は、ステップS 5 5に進む。

ステップS 5 4の処理に進むと、セキュリティモジュール2 3は、不揮発性メモリ4 4に格納しているリストを用いてメモリ記録再生装置4 0 0のID<sub>B</sub>を検証し、その検証をパスしたとき、上記リストをメモリ記録再生装置4 0 0に送信した後、ステップS 5 9の処理に進む。

また、ステップS 5 5の処理に進むと、セキュリティモジュール2 3は、不揮発性メモリ4 4に格納しているリストのバージョンが、メモリ記録再生装置2 0 0が保持するリストのバージョンナンバーよりも大きい（ $A > B$ ）か、或いは等しいか（ $A = B$ ）、或いは小さいか（ $A < B$ ）の判定を行う。このステップS 5 5の判定において、 $A > B$ であると判定した場合、セキュリティモジュール2 3の処理はステップS 5 6に進み、 $A = B$ であると判定した場合、セキュリティモジュール2 3の処理はステップS 5 7に進み、 $A > B$ であると判定した場合、セキュリティモジュール2 3の処理はステップS 5 8に進む。

ステップS 5 6 の処理に進むと、セキュリティモジュール 2 3 は、自己が保持するリストを用いてメモリ記録再生装置 2 0 0 の  $ID_B$  の検証を行い、そのリストをメモリ記録再生装置 1 0 0 に送信した後、ステップS 5 9 に進む。

また、ステップS 5 7 の処理に進むと、セキュリティモジュール 2 3 は、自己が保持するリストを用いてメモリ記録再生装置 2 0 0 の  $ID_B$  の検証を行った後、ステップS 5 9 に進む。

また、ステップS 5 8 の処理に進むと、セキュリティモジュール 2 3 は、メモリ記録再生装置 2 0 0 からリストを受信し、そのバージョンナンバー ( $RevV_B$ ,  $RegV_B$ ) の検証と、当該リストを用いたメモリ記録再生装置 2 0 0 の  $ID_B$  の検証と、センタ  $TC$  のデジタル署名  $TC\text{Sig}$  の検証を行った後、検証が成功であれば自己のリストを送られたリストを用いて更新してステップS 5 9 に進む。

ステップS 5 9 の処理に進むと、セキュリティモジュール 2 3 は、メモリ記録再生装置から記録又は再生の何れの処理が要求されているのか判定する。

当該ステップS 5 9 にて記録の処理が要求されていると判定した場合、セキュリティモジュール 2 3 は、ステップS 6 0 の処理として、メモリ記録再生装置がセッション鍵  $K_{se}$  にて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{se}, K_{co})$  を受信して復号し、次に、その復号により得られた暗号鍵  $K_{co}$  を自己が保持するストレージ鍵  $K_{st}$  で暗号化した値  $E_{nc}(K_{st}, K_{co})$  を生成してメモリ部 2 2 に書き込む。その後、セキュリティモジュール 2 3 は、上記メモリ記録再生装置において上記暗号鍵  $K_{co}$  にて暗号化されたコンテンツデータ  $E_{nc}(K_{co}, \text{data})$  を受信し、メモリ部 2 2 に記録する。

一方、ステップS 5 9にて再生の処理が要求されていると判定した場合、セキュリティモジュール2 3は、ステップS 6 1の処理として、ストレージ鍵Kstにて暗号鍵Kcoが暗号化され例えばメモリ部2 2のデータ記録領域等に記録されている値Enc (Kst, Kco)を読み出して復号し、その復号により得られた暗号鍵Kcoをセッション鍵Kseにて暗号化した値Enc (Kse, Kco)を生成してメモリ記録再生装置に送信する。その後、上記暗号鍵Kcoにて暗号化されているコンテンツデータEnc (Kco, data)は、メモリ部2 2から再生されてメモリ記録再生装置に送られることになる。

〔デバイスタイプ別処理手順〕

次に、前記デバイスタイプDev 1乃至Dev 4に相当する各光ディスク記録再生装置、メモリ記録再生装置における処理の流れを示す。なお、デバイスタイプDev 1に相当する光ディスク記録再生装置3 0 0とデバイスタイプDev 3に相当するメモリ記録再生装置4 0 0の処理の流れは略々同じであり、また、デバイスタイプDev 2に相当する光ディスク記録再生装置1 0 0とデバイスタイプDev 4に相当するメモリ記録再生装置2 0 0の処理の流れは略々同じであるため、以下の説明では、デバイスタイプDev 1及びDev 3での処理と、デバイスタイプDev 2及びDev 4での処理を、それぞれ纏めて説明する。

<デバイスタイプDev 1／Dev 3>

図8 5には、デバイスタイプDev 1及びDev 3の記録再生装置の処理の流れを示す。

この図8 5において、記録再生装置は、ステップS 7 1の処理として、先ず、乱数R<sub>B</sub>を発生して情報記録媒体に送信する。

次に、記録再生装置は、ステップS 7 2の処理として、情報記録媒体から送信されてきた $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$ を受信する。またお、メディア記録再生装置に送信し、 $Cert_A$ の検証、 $Sig_A$ の検証、前記 $V_B = K_B \cdot G$ の計算を行った後、情報記録媒体に対して、 $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$ を送信する。なお、このときバージョンナンバー $RevV_B$ ,  $RegV_B$ は「0」となる。

次に、記録再生装置は、ステップS 7 3の処理として、セッション鍵 $K_{se}$ の計算を行う。

次に、記録再生装置は、ステップS 7 4として、情報記録媒体のメディアタイプが、IM 1か或いはそれ以外(IM 2, IM 3, IM 4)か否かの判定を行う。当該ステップS 7 4の判定において、情報記録媒体がメディアタイプIM 1であると判定した場合、記録再生装置の処理はステップS 7 5に進み、情報記録媒体がメディアタイプIM 1でない(メディアタイプIM 2, IM 3, IM 4)であると判定した場合、記録再生装置の処理はステップS 7 6に進む。

ステップS 7 5の処理に進むと、記録再生装置は、メディアタイプIM 1の光ディスク情報記録媒体5 0の光ディスク1 2からリボケーションリスト及びレジストレーションリストを読み出し、そのリストのバージョンナンバー( $RevV_A$ ,  $RegV_A$ )の検証と、そのリストを用いた光ディスク情報記録媒体5 0の $ID_A$ の検証と、センタTCのデジタル署名 $TC_{Sig}$ の検証を行い、そのリストを光ディスク情報記録媒体5 0のセキュリティモジュール5 3に送信した後、ステップS 7 7に進む。

また、ステップS 7 6の処理に進むと、記録再生装置は、メディ

タイプIM1でないメディアタイプ(IM2乃至IM4)の情報記録媒体のセキュリティモジュールからリボケーションリスト及びレジストレーションリストを受信し、そのリストのバージョンナンバー(RevV<sub>A</sub>, RegV<sub>A</sub>)の検証と、そのリストを用いた情報記録媒体のID<sub>A</sub>の検証と、センタTCのデジタル署名TCSigの検証を行った後、ステップS77に進む。

ステップS77の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

当該ステップS77にて記録の処理を行うと判定した場合、記録再生装置は、ステップS78の処理として、再度、メディアタイプが、IM1, IM2(すなわち光ディスク情報記録媒体)であるか、或いはIM3, IM4(すなわちメモリ情報記録媒体)であるかの判定を行う。当該ステップS78の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS80に進み、情報記録媒体がメディアタイプIM3, IM4であると判定した場合、記録再生装置の処理はステップS81に進む。

また、上記ステップS77にて再生の処理を行うと判定した場合、記録再生装置は、ステップS79の処理として、再度、メディアタイプが、IM1, IM2(光ディスク情報記録媒体)であるか、或いはIM3, IM4(メモリ情報記録媒体)であるかの判定を行う。当該ステップS79の判定において、情報記録媒体がメディアタイプIM1, IM2であると判定した場合、記録再生装置の処理はステップS82に進み、情報記録媒体がメディアタイプIM3, IM



4であると判定した場合、記録再生装置の処理はステップS 8 3に進む。

上記ステップS 8 0の処理に進むと、記録再生装置は、セッション鍵 $K_{se}$ にて暗号鍵 $K_{co}$ を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を送信し、それに対応して情報記録媒体のセキュリティモジュールがストレージ鍵 $K_{st}$ で暗号鍵 $K_{co}$ を暗号化して送信してきた値 $E_{nc}(K_{st}, K_{co})$ を受信した後、ストレージ鍵 $K_{st}$ で暗号鍵 $K_{co}$ を暗号化した値 $E_{nc}(K_{st}, K_{co})$ と暗号鍵 $K_{co}$ でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を情報記録媒体の光ディスクに書き込む。

また、ステップS 8 1の処理に進むと、記録再生装置は、セッション鍵 $K_{se}$ にて暗号鍵 $K_{co}$ を暗号化した値 $E_{nc}(K_{se}, K_{co})$ をセキュリティモジュールに送信した後、暗号鍵 $K_{co}$ でコンテンツデータを暗号化したデータ $E_{nc}(K_{co}, data)$ を送信し、メモリ部に書きこませる。

また、ステップS 8 2の処理に進むと、記録再生装置は、ストレージ鍵 $K_{st}$ にて暗号鍵 $K_{co}$ が暗号化された値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体から読み出し、その値 $E_{nc}(K_{st}, K_{co})$ を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体が値 $E_{nc}(K_{st}, K_{co})$ をストレージ鍵 $K_{st}$ で復号し、さらにその暗号鍵 $K_{co}$ をセッション鍵 $K_{se}$ で暗号化した値 $E_{nc}(K_{se}, K_{co})$ を受信した後、当該暗号鍵 $K_{co}$ で暗号化されているコンテンツデータ $E_{nc}(K_{co}, data)$ を情報記録媒体から読み出す。

また、ステップS 8 3の処理に進むと、記録再生装置は、セッション鍵 $K_{se}$ にて暗号鍵 $K_{co}$ を暗号化した値 $E_{nc}(K_{se}, K_{co})$ を情報記録媒体のセキュリティモジュールから受信した後、当該暗号鍵 $K$

coで暗号化されているコンテンツデータ  $Enc(Kco, data)$  を情報記録媒体のセキュリティモジュールから受信する。

<デバイスタイプ  $Dev2 / Dev4$ >

図86及び図87には、デバイスタイプ  $Dev2$  及び  $Dev4$  の記録再生装置の処理の流れを示す。なお、図86と図87は、本来は1つの図面上に描くべきであるが、紙面の都合で2つの図に分けている。

この図86において、記録再生装置は、ステップS91の処理として、まず、乱数  $R_B$  を発生して情報記録媒体に送信する。

次に、記録再生装置は、ステップS92の処理として、情報記録媒体から送信されてきた  $Cert_A$ ,  $R_A$ ,  $R_B$ ,  $V_A$ ,  $RevV_A$ ,  $RegV_A$ ,  $Sig_A$  を受信する。またお、メディア記録再生装置に送信し、 $Cert_A$  の検証、 $Sig_A$  の検証、前記  $V_B = K_B \cdot G$  の計算を行った後、情報記録媒体に対して、 $Cert_B$ ,  $R_B$ ,  $R_A$ ,  $V_B$ ,  $RevV_B$ ,  $RegV_B$ ,  $Sig_B$  を送信する。

次に、記録再生装置は、ステップS93の処理として、セッション鍵  $K_{se}$  の計算を行う。

次に、記録再生装置は、ステップS94として、情報記録媒体のメディアタイプが、 $IM1$  か或いはそれ以外 ( $IM2$ ,  $IM3$ ,  $IM4$ ) か否かの判定を行う。当該ステップS94の判定において、情報記録媒体がメディアタイプ  $IM1$  であると判定した場合、記録再生装置の処理はステップS95に進み、情報記録媒体がメディアタイプ  $IM1$  でない (メディアタイプ  $IM2$ ,  $IM3$ ,  $IM4$ ) であると判定した場合、記録再生装置の処理はステップS96に進む。

ステップS95の処理に進むと、記録再生装置は、上記  $RevV_A$ ,

RegV<sub>A</sub>と、RevV<sub>B</sub>, RegV<sub>B</sub>からバージョンの新しさの判断を行う。すなわち記録再生装置は、記録媒体が保持するリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい ( $A > B$ ) か、或いは等しいか ( $A = B$ )、或いは小さいか ( $A < B$ ) の判定を行う。このステップS 9 5の判定において、 $A > B$ であると判定した場合、記録再生装置の処理はステップS 9 7に進み、 $A = B$ であると判定した場合、記録再生装置の処理はステップS 9 8に進み、 $A < B$ であると判定した場合、記録再生装置の処理はステップS 9 9に進む。

ステップS 9 7の処理に進むと、記録再生装置は、メディアタイプIM 1の光ディスク情報記録媒体5 0の光ディスク1 2からリボケーションリスト及びレジストレーションリストを読み出し、そのリストのバージョンナンバー (RevV<sub>A</sub>, RegV<sub>A</sub>) の検証と、そのリストを用いた光ディスク情報記録媒体5 0のID<sub>A</sub>の検証と、センタTCのデジタル署名TC Sigの検証を行い、そのリストを光ディスク情報記録媒体5 0のセキュリティモジュール5 3に送信した後、自己のリストを読み出したリストを用いて更新して図8 7のステップS 1 1 0の処理に進む。

また、ステップS 9 8の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID<sub>A</sub>の検証を行い、当該リストを情報記録媒体のセキュリティモジュールに送信した後、図8 7のステップS 1 1 0の処理に進む。

また、ステップS 9 9の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体ID<sub>A</sub>の検証を行い、当該リストを情報記録媒体の送信する。さらに、記録再生装置は、ステップ

S 1 0 3 で、上記情報記録媒体に対して当該リストを書き込みし（更新）た後、図 8 7 のステップ S 1 1 0 の処理に進む。

一方、上記ステップ S 9 6 の処理に進むと、記録再生装置は、上記  $RevV_A$ 、 $RegV_A$  と、 $RevV_B$ 、 $RegV_B$  からバージョンの新しさの判断を行う。すなわち記録再生装置は、情報記録媒体が保持するリストのバージョンが、記録再生装置の保持するバージョンナンバーよりも大きい ( $A > B$ ) か、或いは等しいか ( $A = B$ )、或いは小さいか ( $A < B$ ) の判定を行う。このステップ S 9 6 の判定において、 $A > B$  であると判定した場合、記録再生装置の処理はステップ S 1 0 0 に進み、 $A = B$  であると判定した場合、記録再生装置の処理はステップ S 1 0 1 に進み、 $A < B$  であると判定した場合、記録再生装置の処理はステップ S 1 0 2 に進む。

ステップ S 1 0 0 の処理に進むと、記録再生装置は、メディアタイプ IM 2 乃至 IM 4 の情報記録媒体のセキュリティモジュールからリボケーションリスト及びレジストレーションリストを受信し、そのリストのバージョンナンバー ( $RevV_A$ 、 $RegV_A$ ) の検証と、そのリストを用いた情報記録媒体の  $ID_A$  の検証と、センタ TC のデジタル署名  $TC\text{Sig}$  の検証を行い、検証が成功であれば自己のリストを送られたリストを用いて更新して、図 8 7 のステップ S 1 1 0 の処理に進む。

また、ステップ S 1 0 1 の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体  $ID_A$  の検証を行った後、図 8 7 のステップ S 1 1 0 の処理に進む。

また、ステップ S 1 0 2 の処理に進むと、記録再生装置は、自己が保持するリストを用いて情報記録媒体  $ID_A$  の検証を行い、当該リ

ストを情報記録媒体のセキュリティモジュールに送信した後、図 8 7 のステップ S 1 1 0 の処理に進む。

図 8 7 のステップ S 1 1 0 の処理に進むと、記録再生装置は、情報記録媒体に対してデータの記録を行うのか、或いは情報記録媒体からデータの再生を行うのか判定する。

当該ステップ S 1 1 0 にて記録の処理を行うと判定した場合、記録再生装置は、ステップ S 1 1 1 の処理として、再度、メディアタイプが、IM 1, IM 2 (光ディスク情報記録媒体) であるか、或いは IM 3, IM 4 (メモリ情報記録媒体) であるかの判定を行う。当該ステップ S 1 1 1 の判定において、情報記録媒体がメディアタイプ IM 1, IM 2 であると判定した場合、記録再生装置の処理はステップ S 1 1 3 に進み、情報記録媒体がメディアタイプ IM 3, IM 4 であると判定した場合、記録再生装置の処理はステップ S 1 1 4 に進む。

また、上記ステップ S 1 1 0 にて再生の処理を行うと判定した場合、記録再生装置は、ステップ S 1 1 2 の処理として、再度、メディアタイプが、IM 1, IM 2 (光ディスク情報記録媒体) であるか、或いは IM 3, IM 4 (メモリ情報記録媒体) であるかの判定を行う。当該ステップ S 1 1 2 の判定において、情報記録媒体がメディアタイプ IM 1, IM 2 であると判定した場合、記録再生装置の処理はステップ S 1 1 5 に進み、情報記録媒体がメディアタイプ IM 3, IM 4 であると判定した場合、記録再生装置の処理はステップ S 1 1 6 に進む。

上記ステップ S 1 1 3 の処理に進むと、記録再生装置は、セッション鍵 K<sub>se</sub>にて暗号鍵 K<sub>co</sub>を暗号化した値 E<sub>nc</sub> (K<sub>se</sub>, K<sub>co</sub>) を送信

し、それに対応して情報記録媒体のセキュリティモジュールがストレージ鍵  $K_{st}$  で暗号鍵  $K_{co}$  を暗号化して送信してきた値  $E_{nc}(K_{st}, K_{co})$  を受信した後、ストレージ鍵  $K_{st}$  で暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{st}, K_{co})$  と暗号鍵  $K_{co}$  でコンテンツデータを暗号化したデータ  $E_{nc}(K_{co}, data)$  を情報記録媒体書き込む。

また、ステップ S 1 1 4 の処理に進むと、記録再生装置は、セッション鍵  $K_{se}$  にて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{se}, K_{co})$  をセキュリティモジュールに送信した後、暗号鍵  $K_{co}$  でコンテンツデータを暗号化したデータ  $E_{nc}(K_{co}, data)$  をセキュリティモジュールに送信してメモリ部に記録させる。

また、ステップ S 1 1 5 の処理に進むと、記録再生装置は、ストレージ鍵  $K_{st}$  にて暗号鍵  $K_{co}$  が暗号化された値  $E_{nc}(K_{st}, K_{co})$  を情報記録媒体から読み出し、その値  $E_{nc}(K_{st}, K_{co})$  を情報記録媒体のセキュリティモジュールに送信し、情報記録媒体のセキュリティモジュールが値  $E_{nc}(K_{st}, K_{co})$  をストレージ鍵  $K_{st}$  で復号し、さらにその暗号鍵  $K_{co}$  をセッション鍵  $K_{se}$  で暗号化した値  $E_{nc}(K_{se}, K_{co})$  を受信した後、当該暗号鍵  $K_{co}$  で暗号化されているコンテンツデータ  $E_{nc}(K_{co}, data)$  を情報記録媒体から読み出す。

また、ステップ S 1 1 6 の処理に進むと、記録再生装置は、セッション鍵  $K_{se}$  にて暗号鍵  $K_{co}$  を暗号化した値  $E_{nc}(K_{se}, K_{co})$  を情報記録媒体のセキュリティモジュールから受信した後、当該暗号鍵  $K_{co}$  で暗号化されているコンテンツデータ  $E_{nc}(K_{co}, data)$  を情報記録媒体のセキュリティモジュールから受信する。

なお、上述した実施の形態では、本発明を適用した情報記録媒体として光ディスク記録媒体とメモリ情報記録媒体の例を提示したが、

情報記録媒体はこれに限るものではなく、磁気ディスクや磁気テープ、光磁気ディスク、バッテリーバックアップされた揮発性メモリなどでもよい。

#### 〔記録媒体製造装置及び方法〕

次に、上述した本発明の情報記録媒体を製造する本発明の記録媒体製造装置及び方法について説明する。

以下に、本発明の情報記録媒体として前述した実施の形態のメディアタイプIM1乃至IM4の各情報記録媒体を例に挙げ、それら各メディアタイプIM1乃至IM4の情報記録媒体をそれぞれ製造する記録媒体製造装置について説明を行う。

#### <メディアタイプM1製造>

図88には、後述する記録媒体組立装置700により既に組み立てられているメディアタイプIM1の光ディスク情報記録媒体50に対して、最新のリストを記録する光ディスク(IM1)製造装置500の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

この図88に示す光ディスク製造装置500は、既に組み立てられている光ディスク情報記録媒体50に対してリストを記録するが、上記メディアタイプIM1である光ディスク情報記録媒体50は、前述したようにセキュリティモジュール53がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていない。このため、当該光ディスク製造装置500は、光ディスク情報記録媒体50のコ

ンテンツデータ記録用の領域に上記リストを記録する。

当該光ディスク製造装置 500 は、光ディスク情報記録媒体 50 のカートリッジ 11 内の光ディスク 12 を回転させるスピンドルモータ 501 と、光ディスク 12 のデータ記録領域に情報を少なくとも書き込み可能な光学ヘッド 502 と、スピンドルモータ 501 や光学ヘッド 502 のサーボ回路 503 と、これらを制御する制御部 505 等を備えている。

さらに、光ディスク製造装置 500 は、光ディスク情報記録媒体 50 の ID、プライベート鍵、パブリック鍵証明書、当該媒体 50 の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 507 と、そのドライブ部 606 と、光ディスク情報記録媒体 50 のセキュリティモジュール 53 との間で情報の授受を行うインターフェース部 508 とを備えている。なお、図 88 の構成では、鍵・リスト記録媒体 507 及びドライブ部 506 は、当該光ディスク製造装置 500 に内蔵されている例を挙げているが、当該鍵・リスト記録媒体 507 及びドライブ部 506 は外付けの媒体及びドライブであってもよい。上記 ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びバージョンナンバーは、例えば鍵発行センタ（後述する管理センタ）により発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

上記鍵・リスト記録媒体 507 に格納されている情報は、制御部 505 の制御の元、ドライブ部 506 により読み取られ、当該読み取られた情報のうち、上記 ID、プライベート鍵、パブリック鍵証明書、バージョンナンバーについてはインターフェース部 508 か



ら光ディスク情報記録媒体50のセキュリティモジュール53に送られて記憶され、上記最新のリストは光学ヘッド502にて光ディスク12のデータ記録領域に記録される。

また、ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部509を介して直接に入手することも可能である。このように、外部インターフェース部509を介してID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部509を介したID、プライベート鍵、パブリック鍵証明書、バージョンナンバーは制御部505からインターフェース部508に直接送られて光ディスク情報記録媒体50のセキュリティモジュール53に記憶され、上記最新のリストは制御部505から光学ヘッド502に直接送られて光ディスク12のデータ記録領域に記録されることになる。

図89には、本発明の記録媒体製造方法として、上記メディアタイプIM1の光ディスク情報記録媒体50を製造すると共に、当該メディアタイプIM1の光ディスク情報記録媒体50に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

図89において、光ディスク製造方法では、先ず、ステップS200の製造工程として、後述する記録媒体組立装置700によりメディアタイプIM1の光ディスク情報記録媒体50が組み立てられ

る。

次に、光ディスク製造方法では、ステップS 2 0 1の製造工程として、図88の光ディスク製造装置500により、前記ID、プライベート鍵、パブリック鍵証明書、バージョンナンバーを、メディアタイプIM1である光ディスク情報記録媒体50のセキュリティモジュール53内に設けられている不揮発性の鍵メモリ36に書き込む。

次に、光ディスク製造方法では、ステップS 2 0 2の製造工程として、図88の光ディスク製造装置500により、最新のリストを光ディスク12のコンテンツデータ記録用の領域に書き込む。

以上により、光ディスク情報記録媒体50は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

#### <メディアタイプM2製造>

図90には、後述する記録媒体組立装置700により既に組み立てられているメディアタイプIM2の光ディスク情報記録媒体10に対して、最新のリストを記録する光ディスク(IM2)製造装置510の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであってても良い。

この図90に示す光ディスク製造装置510は、既に組み立てられている光ディスク情報記録媒体10に対して、リストを記録するが、上記メディアタイプIM2である光ディスク情報記録媒体10は、前述したようにセキュリティモジュール13がリストを格納す

るための十分な記憶容量を有する不揮発性メモリ（３４）を備えている。このため、当該光ディスク製造装置５１０は、光ディスク情報記録媒体１０のセキュリティモジュール１３の不揮発性メモリに上記リストを記録する。

当該光ディスク製造装置５１０は、少なくとも、光ディスク情報記録媒体１０のセキュリティモジュール１３にリストを送信するためのインターフェース部５１８と、各部を制御する制御部５１５等を備えている。なお、図９０の例では、図５８の例のようにスピンドルモータや光学ヘッド等を備えていない構成を挙げているが、光ディスク製造装置５１０はもちろんそれらを備えていてもよい。

さらに、光ディスク製造装置５１０は、光ディスク情報記録媒体１０のＩＤ、プライベート鍵、パブリック鍵証明書、当該媒体１０の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体５１７とそのドライブ部５１６も備えている。なお、図９０の構成では、鍵・リスト記録媒体５１７及びドライブ部５１６は、当該光ディスク製造装置５１０に内蔵されている例を挙げているが、当該鍵・リスト記録媒体５１７及びドライブ部５１６は外付けの媒体及びドライブであってもよい。上記ＩＤ、プライベート鍵、パブリック鍵証明書、最新のリスト及びバージョンナンバーは、鍵発行センタ（後述する管理センタ）により発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

上記鍵・リスト記録媒体５１７に格納されている情報は、制御部５１５の制御の元、ドライブ部５１６により読み取られ、インターフェース部５１８から光ディスク情報記録媒体１０のセキュリティ

モジュール 13 に送られて不揮発性メモリ (34) に記憶される。

また、この図 90 の例でも前記図 88 の場合と同様に、ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、鍵発行センタより送られてきたものを外部インターフェース部 519 を介して直接に入手することも可能である。外部インターフェース部 519 を介して ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部 519 を介した ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部 515 からインターフェース部 518 に直接送られて光ディスク情報記録媒体 10 のセキュリティモジュール 13 に送られて不揮発性メモリ 34 に記録されることになる。

図 91 には、本発明の記録媒体製造方法として、上記メディアタイプ IM2 の光ディスク情報記録媒体 10 を製造すると共に、当該光ディスク情報記録媒体 10 に対して最新のリストを記録する光ディスク製造方法における製造工程の流れを示す。

図 91 において、光ディスク製造方法では、先ず、ステップ S210 の製造工程として、後述する記録媒体組立装置 700 によりメディアタイプ IM2 の光ディスク情報記録媒体 10 が組み立てられる。

次に、光ディスク製造方法では、ステップ S211 の製造工程として、図 90 の光ディスク製造装置 510 により、前記 ID、プライベート鍵、パブリック鍵証明書、バージョンナンバーを、メディ

アタイプIM2である光ディスク情報記録媒体10のセキュリティモジュール13内に設けられている不揮発性メモリ34に書き込む。

次に、光ディスク製造方法では、ステップS212の製造工程として、図90の光ディスク製造装置510により、最新のリストを光ディスク情報記録媒体10のセキュリティモジュール13内に設けられている不揮発性メモリ34に書き込む。

以上により、光ディスク記録再生装置10は、セキュリティモジュール13に最新版のリストを記録した状態で製造工場から出荷されることになる。

#### <メディアタイプIM3製造>

図92には、後述する記録媒体組立装置700により既に組み立てられているメディアタイプIM3のメモリ情報記録媒体60に対して、最新のリストを記録するメモリ(IM3)製造装置600の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。

この図92に示すメモリ製造装置600は、既に組み立てられているメモリ情報記録媒体60に対して、リストを記録するが、上記メディアタイプIM3であるメモリ情報記録媒体60は、前述したようにセキュリティモジュール63がリストを格納するための不揮発性メモリを備えていないか、或いは不揮発性メモリがリストを格納するのに十分な記憶容量を備えていない。このため、当該メモリ製造装置600は、メモリ情報記録媒体60のメモリ部22のコンテンツデータ記録用の領域に上記リストを記録する。

当該メモリ製造装置 600 は、少なくとも、メモリ情報記録媒体 60 に信号を送信するためのインターフェース部 608 と、メモリ情報記録媒体 60 の入出力端子 24 に接続するための入出力端子 601 と、各部を制御する制御部 605 等を備えている。

さらに、メモリ製造装置 600 は、メモリ情報記録媒体 60 の ID、プライベート鍵、パブリック鍵証明書、当該媒体 60 の製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 607 とそのドライブ部 606 を備えている。なお、図 92 の構成では、鍵・リスト記録媒体 607 及びドライブ部 606 は、当該メモリ製造装置 600 に内蔵されている例を挙げているが、当該鍵・リスト記録媒体 607 及びドライブ部 606 は外付けの媒体及びドライブであってもよい。上記 ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びバージョンナンバーは、鍵発行センタ（後述する管理センタ）により発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

上記鍵・リスト記録媒体 607 に格納されている情報は、制御部 605 の制御の元、ドライブ部 606 により読み取られ、インターフェース部 608 及び入出力端子 601 を介して、メモリ情報記録媒体 60 に送られる。このときのメモリ情報記録媒体 60 では、メモリ製造装置 600 から送られてきた上記 ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを、メモリ部 22 のデータ記録領域に記録する。

また、ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、上述したように内蔵或いは外付

けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタより送られてきたものを外部インターフェース部609を介して直接に入手することも可能である。このように、外部インターフェース部609を介してID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部609を介したID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、制御部605からインターフェース部608、入出力端子601を介して直接メモリ情報記録媒体60に送られ、メモリ部22のデータ記録領域に記録されることになる。

図93には、本発明の記録媒体製造方法として、上記メディアタイプIM3のメモリ情報記録媒体60を製造すると共に、当該メモリ情報記録媒体60に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

図93において、メモリ製造方法では、まず、ステップS300の製造工程として、後述する記録媒体組立装置700によりメディアタイプIM3のメモリ情報記録媒体60が組み立てられる。

次に、メモリ製造方法では、ステップS301の製造工程として、図92のメモリ製造装置600により、前記ID、プライベート鍵、パブリック鍵証明書、バージョンナンバーを、メディアタイプIM3であるメモリ情報記録媒体60のメモリ部22のデータ記録領域に書き込む。

次に、メモリ製造方法では、ステップS302の製造工程として、図92のメモリ製造装置600により、最新のリストをメモリ部2

2 のコンテンツデータ記録用の領域に書き込む。

以上により、メモリ情報記録媒体 60 は、最新版のリストをデータ記録領域に記録した状態で製造工場から出荷されることになる。

#### <メディアタイプ IM4 製造>

図 94 には、後述する記録媒体組立装置 700 により既に組み立てられているメディアタイプ IM4 のメモリ情報記録媒体 20 に対して、最新のリストを記録するメモリ (IM4) 製造装置 610 の概略構成を示す。なお、記録する最新のリストは、リボケーションリスト又はレジストレーションリストの一方、或いは、リボケーションリスト及びレジストレーションリストの両方の何れであっても良い。この図 94 において、図 92 と同じ構成要素にはそれぞれ同一の指示符号を付している。

この図 94 に示すメモリ製造装置 610 は、既に組み立てられているメモリ情報記録媒体 20 に対して、リストを記録するが、上記メディアタイプ IM4 であるメモリ情報記録媒体 20 は、前述したようにセキュリティモジュール 23 がリストを格納するための十分な記憶容量を有する不揮発性メモリ (44) を備えている。このため、当該メモリ製造装置 610 は、メモリ情報記録媒体 20 のセキュリティモジュール 23 内の不揮発性メモリに上記リストを記録する。

当該メモリ製造装置 610 は、メモリ情報記録媒体 20 に信号を送信するためのインターフェース部 618 と、メモリ情報記録媒体 20 の入出力端子 24 に接続するための入出力端子 601 と、各部を制御する制御部 605 等を備え、さらに、メモリ情報記録媒体 20 の ID、プライベート鍵、パブリック鍵証明書、当該媒体 20 の



製造時点における最新のリスト及びそのバージョンナンバーを予め格納している鍵・リスト記録媒体 607 とそのドライブ部 606 を備えている。なお、この図 94 の場合も前記図 92 の例と同様に、当該鍵・リスト記録媒体 607 及びドライブ部 606 は外付けの媒体及びドライブであってもよい。上記 ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びバージョンナンバーは、鍵発行センタ（後述する管理センタ）により発行されるものであり、上記内蔵或いは外付けの鍵・リスト記録媒体に予め格納されている。

上記鍵・リスト記録媒体 607 に格納されている情報は、制御部 605 の制御の下、ドライブ部 606 により読み取られ、インターフェース部 608 及び入出力端子 601 を介して、メモリ情報記録媒体 20 に送られる。このときのメモリ情報記録媒体 20 では、メモリ製造装置 610 から送られてきた上記 ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを、セキュリティモジュール 23 の不揮発性メモリ（44）に記録する。

またこの図 94 の例においても前記図 92 の例と同様に、ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーは、上述した内蔵或いは外付けの鍵・リスト記録媒体に予め格納されているものを読み取るだけでなく、例えば鍵発行センタ（後述する管理センタ）より送られてきたものを外部インターフェース部 609 を介して直接に入手することも可能である。このように、外部インターフェース部 609 を介して ID、プライベート鍵、パブリック鍵証明書、最新のリスト及びそのバージョンナンバーを入手するようにした場合、当該外部インターフェース部 609 を介した ID、プライベート鍵、パブリック鍵証明書、最新の

リスト及びそのバージョンナンバーは、制御部605からインターフェース部608、入出力端子601を介して直接メモリ情報記録媒体20に送られ、セキュリティモジュール23内の不揮発性メモリ(44)に記録されることになる。

図95には、本発明の記録媒体製造方法として、上記メディアタイプIM4のメモリ情報記録媒体20を製造すると共に、当該メモリ情報記録媒体20に対して最新のリストを記録するメモリ製造方法における製造工程の流れを示す。

図95において、メモリ製造方法では、まず、ステップS310の製造工程として、後述する記録媒体組立装置700によりメディアタイプIM4のメモリ情報記録媒体20が組み立てられる。

次に、メモリ製造方法では、ステップS311の製造工程として、図94のメモリ製造装置610により、前記ID、プライベート鍵、パブリック鍵証明書、バージョンナンバーを、メディアタイプIM4であるメモリ情報記録媒体20のセキュリティモジュール23内の不揮発性メモリ44に書き込む。

次に、メモリ製造方法では、ステップS312の製造工程として、図94のメモリ製造装置610により、最新のリストをメモリ情報記録媒体20のセキュリティモジュール23内の不揮発性メモリ44に書き込む。

以上により、メモリ情報記録媒体20は、最新版のリストをセキュリティモジュール23の不揮発性メモリ44に記録した状態で製造工場から出荷されることになる。

#### <製造装置の構成>

次に、上述したメディアタイプIM1，IM2の光ディスク情報

記録媒体、メディアタイプIM3, IM4のメモリ情報記録媒体を製造する製造装置の概略構成を図96に示す。

この図96に示す製造装置は、大別して、記録媒体組立装置700と情報書き込み装置710とからなる。上記記録媒体組立装置700は、上記メディアタイプIM1乃至IM4の情報記録媒体を構成する各部品等を元にそれら情報記録媒体を組み立てる。上記情報書き込み装置710は、記録媒体組立装置700により組み立てられた記録媒体が例えば搬送及び装填され、それら各情報記録媒体のメディアタイプに応じて、前記最新のリストや鍵等の情報を書き込む。

なお、記録媒体組立装置700は、必ずしも全てのメディアタイプの情報記録媒体を製造する必要はなく、所望のメディアタイプの情報記録媒体のみ組み立てるものであってもよく、また、情報書き込み装置710においても同様に、必ずしも全てのメディアタイプの情報記録媒体に情報を書き込むものである必要はなく、所望のメディアタイプの情報記録媒体のみに情報を書き込むものであっても良いが、ここでは全てのメディアタイプの情報記録媒体の組み立てと情報の書き込むを行う例を挙げている。さらに、記録媒体の組立工程が複数の工程に分散しているような場合、上記情報記録媒体組立装置700は、それら各組立工程にて使用される全ての組立装置を含むものである。

上記情報書き込み装置710は、光ディスク製造装置500と、光ディスク製造装置510と、メモリ製造装置600と、メモリ製造装置610とを有し、また、制御管理装置711と、操作パネル713と、モニタ714と、情報蓄積装置715等をも備えている。

上記光ディスク製造装置 500 は、前述の図 88 に示した装置であり、メディアタイプ IM1 の光ディスク情報記録媒体 50 に対して最新のリスト等を記録する。光ディスク製造装置 510 は、前述の図 90 に示した装置であり、メディアタイプ IM2 の光ディスク情報記録媒体 10 に対して最新のリスト等を記録する。メモリ製造装置 600 は、前述の図 92 に示した装置であり、メディアタイプ IM3 のメモリ情報記録媒体 60 に対して最新のリスト等を記録する。メモリ製造装置 610 は、前述の図 94 に示した装置であり、メディアタイプ IM4 のメモリ情報記録媒体 20 に対して最新のリスト等を記録する。

また、上記制御管理装置 711 は、上記各製造装置 500, 510, 600, 610 の動作及び上記最新のリストや鍵等の情報の書き込み動作を所定のプログラムに基づいて制御すると共に、それら各製造装置 500, 510, 600, 610 に装填された各情報記録媒体 50, 10, 60, 20 の ID 等の管理を行う。上記操作パネル 713 は、上記制御管理装置 711 の制御パラメータ等を例えば使用者が設定等する際に操作されるものであり、上記モニタ 714 は、当該情報書き込み装置 710 の動作状況等を表示するためのものである。

さらに、上記情報蓄積装置 715 には、前記センタ TC、鍵発行センタとしての管理センタ 720 から供給された、最新のリボケーションリスト及びレジストレーションリストやパブリック鍵証明書などを蓄積する。当該情報蓄積装置 715 からは、上記制御管理装置 711 の要求に応じたリストや鍵等の情報が読み出され、当該制御管理装置 711 を介して各製造装置 500, 510, 600, 6

10に送られる。これにより、各製造装置500, 510, 600, 610では、それぞれ装填されている情報記録媒体50, 10, 60, 20に対して最新のリストや鍵等の情報が書き込まれることになる。

なお、この図96の説明では、各情報記録媒体50, 10, 60, 20の組立終了後に、上記最新のリスト等の書き込みが行われる例を挙げているが、各情報記録媒体に組み込まれる前のセキュリティモジュールに対して、上記リストや鍵（メディアタイプに応じた情報）を書き込み、その後に情報記録媒体に組み込むようにしても良い。

#### 産業上の利用可能性

以上に説明したように、本発明によれば、記録媒体にセキュリティモジュールを持たせ、記録媒体上に記録されるデータは個々のデータ毎に異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管することができる。

また、本発明において、セキュリティモジュールは、データの記録時及び再生時に、記録再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにすることができる。

さらに、本発明によれば、信頼できるセンタが発行するリボケーションリスト及び／又はレジストレーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしま

った装置にデータを与えることも防ぐことが可能となる。

このため、本発明によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことが可能である。

## 請求の範囲

1. データを記録する情報記録媒体と前記情報記録媒体にアクセスするドライブ装置とを有する情報伝達システムにおいて、

前記情報記録媒体は、

前記ドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、

データを記録する記録媒体とを具備し、

前記ドライブ装置は、

前記情報記録媒体へのアクセス時に相互認証プロトコルを実行する制御部と、

前記情報記録媒体の記録媒体にアクセスするインターフェース部とを具備することを特徴とする情報伝達システム。

2. 前記相互認証プロトコルは、公開鍵暗号技術を用いたプロトコルであることを特徴とする請求項 1 記載の情報伝達システム。

3. 前記情報記録媒体は、前記セキュリティモジュールと前記記録媒体であるディスクとを具備することを特徴とする請求項 1 記載の情報伝達システム。

4. 前記ドライブ装置は、前記情報記録媒体の記録媒体であるディスクを駆動する駆動部を更に具備することを特徴とする請求項 3 記載の情報伝達システム。

5. インターフェース部は、直接、前記記録媒体にアクセスすることを特徴とする請求項 1 記載の情報伝達システム。

6. 前記情報記録媒体は、前記セキュリティモジュールと前記記録媒体であるメモリチップとを具備することを特徴とする請求項 1 記

載の情報伝達システム。

7. インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスすることを特徴とする請求項1記載の情報伝達システム。

8. 前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶しており、

前記ドライブ装置は、その内部に自己を識別する為の識別情報を記憶している記憶部を更に具備し、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記識別情報を交換し、互いに相手の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項1記載の情報伝達システム。

9. 前記情報記録媒体の識別情報は、前記セキュリティモジュール内に記憶されていることを特徴とする請求項8記載の情報伝達システム。

10. 前記情報記録媒体は、前記リストを前記セキュリティモジュール内に記憶していることを特徴とする請求項8記載の情報伝達システム。

11. 前記情報記録媒体は、前記リストを前記記録媒体内に記憶していることを特徴とする請求項8記載の情報伝達システム。

12. 前記ドライブ装置は、前記記憶部に前記リストを記憶していることを特徴とする請求項8記載の情報伝達システム。

13. 前記ドライブ装置は、前記リストを記憶していないことを特



徴とする請求項 8 記載の情報伝達システム。

14. 前記セキュリティモジュールと前記ドライブ装置の何れか一方若しくは両方がリストを保持するか否かに応じた相互認証プロトコルを実行することを特徴とする請求項 8 記載の情報伝達システム。

15. 前記ドライブ装置の制御部は、前記セキュリティモジュールが前記リストを記憶している前記情報記録媒体か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 8 記載の情報伝達システム。

16. 前記情報記録媒体のセキュリティモジュールは、前記リストを記憶している前記ドライブ装置か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 8 記載の情報伝達システム。

17. 前記情報記録媒体は、その内部に前記リストのバージョン番号及びリストを記憶しており、

前記ドライブ装置は、前記記憶部にその内部に前記リストのバージョン番号及びリストを記憶しており、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、新しいリストを持つ方が、それを他方に送り、古いリストを持つものは送られた新しいリストを用いて自分のリストを更新することを特徴とする請求項 8 記載の情報伝達システム。

18. 前記情報記録媒体は、その内部に前記リストのバージョン番号を記憶しており、かつ、前記記録媒体上にリストが記録されており、

前記ドライブ装置は、前記記憶部にその内部に前記リストのバージョン番号及びリストを記憶しており、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、

前記ドライブ装置は、自己のリストが新しい場合には、自己のリストを前記情報記録媒体に書き込み、自己のリストが古い場合には、前記情報記録媒体からリストを読み出し、読み出したリストを用いて自分のリストを更新することを特徴とする請求項 8 記載の情報伝達システム。

19. 前記ドライブ装置及び前記セキュリティモジュールは、共に上記新しいリストを用いて、相手の識別情報がリストに登録されているか否かを確認することを特徴とする請求項 8 記載の情報伝達システム。

20. 前記ドライブ装置は、その内部に自己を識別する為の識別情報を記憶している記憶部を更に具備し、

前記情報記録媒体のセキュリティモジュールは、前記相互認証プロトコル処理時に、前記識別情報を前記ドライブ装置から受信し、前記ドライブ装置の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 1 記載の情報伝達システム。

21. 前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶しており、

前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、

前記識別情報を前記セキュリティモジュールから受信し、前記セキュリティモジュールの識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 1 記載の情報伝達システム。

22. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリストであり、このリストに登録されている機器を排除すべき機器とすることを特徴とする請求項 8、請求項 20 又は請求項 21 記載の情報伝達システム。

23. 前記不正な機器を排除するためのリストは、排除すべきでない機器の識別情報が登録されたリストであり、このリストに登録されていない機器を排除すべき機器とすることを特徴とする請求項 8、請求項 20 又は請求項 21 記載の情報伝達システム。

24. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、リボケーションリストに登録されている、及び／又は、レジストレーションリストに登録されていない機器を排除すべき機器とすることを特徴とする請求項 8、請求項 20 又は請求項 21 記載の情報伝達システム。

25. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、前記リボケーションリストとレジストレーションリストのうち何れか一方を選択的に、排除すべき機器となっているか

否かを判定することを特徴とする請求項 8、請求項 20 又は請求項 21 記載の情報伝達システム。

26. 前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を暗号化して一方から他方に送ることを特徴とする請求項 1 記載の情報伝達システム。

27. 前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化して一方から他方に送ることを特徴とする請求項 1 記載の情報伝達システム。

28. 前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いて、データを暗号化する暗号鍵を暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、

前記ドライブ装置は、前記暗号鍵で暗号化されたデータと前記セキュリティモジュールによって保存鍵で暗号化された暗号鍵を前記インターフェース部を介して記録媒体に記録することを特徴とす

る請求項 1 記載の情報伝達システム。

29. 前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、暗号化された暗号鍵を前記記録媒体から読み出し、前記読み出された暗号鍵を前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて、復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵で暗号化されたデータを前記記録媒体から読み出して復号することを特徴とする請求項 1 記載の情報伝達システム。

30. 前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用

いて暗号化した、データを暗号化する暗号鍵と前記暗号鍵を用いて暗号化したデータとを前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いてを再度暗号化した暗号鍵と、前記ドライブ装置から受信した前記暗号鍵を用いて暗号化したデータとを前記記録媒体に記録することを特徴とする請求項 1 記載の情報伝達システム。

3 1. 前記ドライブ装置は、前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、  
前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いてデータを暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化されたデータを共有された鍵を用いて復号し、暗号鍵を用いて、復号したデータを暗号化して記録媒体に格納することを特徴とする請求項 1 記載の情報伝達システム。

3 2. 前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を

用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールは、暗号化された暗号鍵と前記暗号鍵を用いて暗号化されたデータとを前記記録媒体から読出し、前記暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて再度暗号化した暗号鍵と前記記録媒体から読み出した暗号鍵で暗号化されたデータを前記ドライブ装置に送り、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵を用いて、暗号化されたデータを復号することを特徴とする請求項 1 記載の情報伝達システム。

33. 前記ドライブ装置は、前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールは、暗号化されて情報記録媒体に格納されているデータを読み出すと共に、暗号鍵を用いて暗号化されたデータを復号し、前記鍵共有プロトコルによって共有した鍵を用いて、復号されたデータを再度暗号化してドライブ装置に送り、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化されたデータを復号することを特徴とする請求項 1 記載の情報伝達システム。

34. データを記録する記録媒体を備えた情報記録媒体と、前記情報記録媒体にアクセスするドライブ装置との間で情報を伝達を行う際の情報伝達方法において、

前記ドライブ装置が備える制御部と前記情報記録媒体が備えるセキュリティモジュールとの間で相互認証プロトコルを実行し、

前記相互認証プロトコルの認証結果に応じて、前記ドライブ装置が前記情報記録媒体の記録媒体へアクセスすることを特徴とする情報伝達方法。

35. 前記相互認証プロトコルは、公開鍵暗号技術を用いたプロトコルであることを特徴とする請求項34記載の情報伝達方法。

36. 前記ドライブ装置が備えるインターフェース部は、直接、前記記録媒体にアクセスすることを特徴とする請求項34記載の情報伝達方法。

37. 前記ドライブ装置が備えるインターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスすることを特徴とする請求項34記載の情報伝達方法。

38. 前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶し、

前記ドライブ装置が備える記憶部は、その内部に自己を識別する為の識別情報を記憶し、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記情報記録媒体の識別情報と前記ドライブ装置の識別情報を交換し、互いに相手の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には相互認証プ



ロトコルの以後のプロセスを行わないことを特徴とする請求項 3 4 記載の情報伝達方法。

3 9 . 前記情報記録媒体のセキュリティモジュールは、前記識別情報を記憶していることを特徴とする請求項 3 8 記載の情報伝達方法。

4 0 . 前記情報記録媒体のセキュリティモジュールは、前記リストを記憶していることを特徴とする請求項 3 8 記載の情報伝達方法。

4 1 . 前記情報記録媒体の前記記録媒体は、前記リストを記憶していることを特徴とする請求項 3 8 記載の情報伝達方法。

4 2 . 前記ドライブ装置の記憶部は、前記リストを記憶していることを特徴とする請求項 3 8 記載の情報伝達方法。

4 3 . 前記ドライブ装置は、前記リストを記憶していないことを特徴とする請求項 3 8 記載の情報伝達方法。

4 4 . 前記セキュリティモジュールと前記ドライブ装置の何れか一方若しくは両方がリストを保持するか否かに応じた相互認証プロトコルを実行することを特徴とする請求項 3 8 記載の情報伝達方法。

4 5 . 前記ドライブ装置の制御部は、前記セキュリティモジュールが前記リストを記憶している前記情報記録媒体か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 3 8 記載の情報伝達方法。

4 6 . 前記情報記録媒体のセキュリティモジュールは、前記リストを記憶している否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 3 8 記載の情報伝達方法。

4 7 . 前記情報記録媒体は、その内部に前記リストのバージョン番号及びリストを記憶し、

前記ドライブ装置が備える記憶部は、その内部に前記リストのバージョン番号及びリストを記憶し、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、新しいリストを持つ方が、それを他方に送り、古いリストを持つものは送られた新しいリストを用いて自分のリストを更新することを特徴とする請求項 38 記載の情報伝達方法。

48. 前記情報記録媒体は、その内部に前記リストのバージョン番号を記憶し、かつ、前記記録媒体上にリストが記録され、

前記ドライブ装置が備える記憶部は、その内部に前記リストのバージョン番号及びリストを記憶し、

前記情報記録媒体のセキュリティモジュール及び前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記リストのバージョン番号を交換し、

前記ドライブ装置は、自己のリストが新しい場合には、自己のリストを前記情報記録媒体に書き込み、自己のリストが古い場合には、前記情報記録媒体からリストを読み出し、読み出したリストを用いて自分のリストを更新することを特徴とする請求項 38 記載の情報伝達方法。

49. 前記ドライブ装置及び前記セキュリティモジュールは、共に上記新しいリストを用いて、相手の識別情報がリストに登録されているか否かを確認することを特徴とする請求項 38 記載の情報伝達方法。

50. 前記ドライブ装置が備える記憶部は、その内部に自己を識別する為の識別情報を記憶し、

前記情報記録媒体のセキュリティモジュールは、前記相互認証プロトコル処理時に、前記識別情報を前記ドライブ装置から受信し、前記ドライブ装置の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 3 4 記載の情報伝達方法。

5 1 . 前記情報記録媒体は、その内部に自己を識別する為の識別情報を記憶し、

前記ドライブ装置の制御部は、前記相互認証プロトコル処理時に、前記識別情報を前記セキュリティモジュールから受信し、前記セキュリティモジュールの識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 3 4 記載の情報伝達方法。

5 2 . 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリストであり、このリストに登録されている機器を排除すべき機器とすることを特徴とする請求項 3 8、請求項 5 0 又は請求項 5 1 記載の情報伝達方法。

5 3 . 前記不正な機器を排除するためのリストは、排除すべきでない機器の識別情報が登録されたリストであり、このリストに登録されていない機器を排除すべき機器とする請求項 3 8、請求項 5 0 又は請求項 5 1 記載の情報伝達方法。

5 4 . 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成

されており、リボケーションリストに登録されている、及び／又は、レジストレーションリストに登録されていない機器を排除すべき機器とすることを特徴とする請求項 38、請求項 50 又は請求項 51 記載の情報伝達方法。

55. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、前記リボケーションリストとレジストレーションリストのうち何れか一方を選択的に、排除すべき機器となっているか否かを判定することを特徴とする請求項 38、請求項 50 又は請求項 51 記載の情報伝達方法。

56. 前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を暗号化して一方から他方に送ることを特徴とする請求項 34 記載の情報伝達方法。

57. 前記相互認証プロトコルを実行時に、上記ドライブ装置とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化して一方から他方に送ることを特徴とする請求項 34 記載の情報伝達方法。

58. 前記ドライブ装置は、データを前記記録媒体に記録する処理を行う装置であり、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用

いて、データを暗号化する暗号鍵を暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、

前記ドライブ装置は、前記暗号鍵で暗号化されたデータと前記セキュリティモジュールによって保存鍵で暗号化された暗号鍵を記録媒体に記録することを特徴とする請求項 3 4 記載の情報伝達方法。

5 9. 前記ドライブ装置は、暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、暗号化された暗号鍵を前記記録媒体から読み出し、前記読み出された暗号鍵を前記セキュリティモジュールに送り、

前記セキュリティモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて、復号された暗号鍵を再度暗号化して前記ドライブ装置に送信し、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵で暗号化されたデータを前記記録媒体から読み出して復号することを特徴とする請求項 3 4 記載の情報伝

達方法。

60. 前記ドライブ装置は、インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティーモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いて暗号化した、データを暗号化する暗号鍵と前記暗号鍵を用いて暗号化したデータとを前記セキュリティーモジュールに送り、

前記セキュリティーモジュールは、前記ドライブ装置から受信した暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティーモジュールに記憶された保存鍵を用いてを再度暗号化した暗号鍵と、前記ドライブ装置から受信した前記暗号鍵を用いて暗号化したデータとを前記記録媒体に記録することを特徴とする請求項34記載の情報伝達方法。

61. 前記ドライブ装置は、インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティーモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記ドライブ装置は、鍵共有プロトコルによって共有した鍵を用いてデータを暗号化して前記セキュリティーモジュールに送り、

前記セキュリティーモジュールは、前記ドライブ装置から受信した

暗号化されたデータを共有された鍵を用いて復号し、暗号鍵を用いて、復号したデータを暗号化して記録媒体に格納することを特徴とする請求項 3 4 記載の情報伝達方法。

6 2. 前記ドライブ装置は、インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールは、暗号化された暗号鍵と前記暗号鍵を用いて暗号化されたデータとを前記記録媒体から読出し、前記暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて再度暗号化した暗号鍵と前記記録媒体から読み出した暗号鍵で暗号化されたデータを前記ドライブ装置に送り、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵を用いて、暗号化されたデータを復号することを特徴とする請求項 3 4 記載の情報伝達方法。

6 3. 前記ドライブ装置は、インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記ドライブ装置と前記セキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールは、暗号化されて情報記録媒体に格納されているデータを読み出すと共に、暗号鍵を用いて暗号化されたデータを復号し、前記鍵共有プロトコルによって共有した鍵を用いて、復号されたデータを再度暗号化してドライブ装置に送り、

前記ドライブ装置は、鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化されたデータを復号することを特徴とする請求項 3 4 記載の情報伝達方法。

6 4 . データを記録する記録媒体と、ドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールとを具備する情報記録媒体に、アクセスするドライブ装置であって、

前記情報記録媒体へのアクセス時に相互認証プロトコルを実行する制御部と、

前記情報記録媒体の記録媒体にアクセスするインターフェース部とを具備することを特徴とするドライブ装置。

6 5 . 前記相互認証プロトコルは、公開鍵暗号技術を用いたプロトコルであることを特徴とする請求項 6 4 記載のドライブ装置。

6 6 . 前記情報記録媒体の記録媒体であるディスクを駆動する駆動部を更に具備することを特徴とする請求項 6 4 記載のドライブ装置。

6 7 . 前記インターフェース部は、前記情報記録媒体の記録媒体であるメモリチップにアクセスすることを特徴とする請求項 6 4 記載のドライブ装置。

6 8 . インターフェース部は、直接、前記記録媒体にアクセスすることを特徴とする請求項 6 4 記載のドライブ装置。

6 9 . 前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスすることを特徴とする



請求項 6 4 記載のドライブ装置。

7 0 . 自己を識別する為の識別情報を記憶している記憶部を更に具備し、

前記制御部は、前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持している当該情報記録媒体を識別するための識別情報と、前記記憶部に記憶している識別情報を交換し、前記セキュリティモジュールとの間で前記識別情報を交換し、互いに相手の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 6 4 記載のドライブ装置。

7 1 . 前記記憶部に前記リストを記憶していることを特徴とする請求項 7 0 記載のドライブ装置。

7 2 . 前記リストを記憶していないことを特徴とする請求項 7 0 記載のドライブ装置。

7 3 . 前記セキュリティモジュールと自己の何れか一方若しくは両方がリストを保持するか否かに応じた相互認証プロトコルを実行することを特徴とする請求項 7 0 記載のドライブ装置。

7 4 . 前記制御部は、前記セキュリティモジュールが前記リストを記憶している前記情報記録媒体か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 7 0 記載のドライブ装置。

7 5 . 前記記憶部に前記リストのバージョン番号及びリストを記憶しており、

前記制御部は、前記相互認証プロトコル処理時に、前記情報記録

媒体がその内部に保持するリストのバージョン番号と前記記憶部に記憶している前記リストのバージョン番号を交換し、自己が新しいリストを持つときそれをセキュリティモジュールに送り、自己が古いリストを持つときはセキュリティモジュールから送られた新しいリストを用いて自分のリストを更新することを特徴とする請求項 70 記載のドライブ装置。

76. 前記記憶部に前記リストのバージョン番号及びリストを記憶しており、

前記制御部は、前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持するリストのバージョン番号と前記記憶部に記憶している前記リストのバージョン番号を交換し、自己のリストが新しい場合には、自己のリストを前記情報記録媒体の記録媒体上に書き込み、自己のリストが古い場合には、前記情報記録媒体の記録媒体上に記録されているリストを読み出し、読み出したリストを用いて自分のリストを更新することを特徴とする請求項 70 記載のドライブ装置。

77. 前記セキュリティモジュールとの間で、共に上記新しいリストを用いて、相手の識別情報がリストに登録されているか否かを確認することを特徴とする請求項 70 記載のドライブ装置。

78. 前記制御部は、前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持している当該情報記録媒体を識別するための識別情報を前記セキュリティモジュールから受信し、前記セキュリティモジュールの識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを

特徴とする請求項 6 4 記載のドライブ装置。

7 9. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリストであり、このリストに登録されている機器を排除すべき機器とすることを特徴とする請求項 7 0 又は請求項 7 8 記載のドライブ装置。

8 0. 前記不正な機器を排除するためのリストは、排除すべきでない機器の識別情報が登録されたリストであり、このリストに登録されていない機器を排除すべき機器とする請求項 7 0 又は請求項 7 8 記載のドライブ装置。

8 1. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、リボケーションリストに登録されている、及び／又は、レジストレーションリストに登録されていない機器を排除すべき機器とすることを特徴とする請求項 7 0 又は請求項 7 8 記載のドライブ装置。

8 2. 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、前記リボケーションリストとレジストレーションリストのうち何れか一方を選択的に、排除すべき機器となっているか否かを判定することを特徴とする請求項 7 0 又は請求項 7 8 記載のドライブ装置。

8 3. 前記相互認証プロトコルを実行時に、自己と前記セキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、

共有された鍵を用いてデータを暗号化する暗号鍵を暗号化して一方から他方に送ることを特徴とする請求項 6 4 記載のドライブ装置。

8 4 . 前記相互認証プロトコルを実行時に、自己とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化して一方から他方に送ることを特徴とする請求項 6 4 記載のドライブ装置。

8 5 . 前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記鍵共有プロトコルによって共有した鍵を用いて、データを暗号化する暗号鍵を暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて復号された暗号鍵を再度暗号化したデータを受信し、

前記暗号鍵で暗号化されたデータと前記セキュリティモジュールによって保存鍵で暗号化された暗号鍵を前記インターフェース部を介して記録媒体に記録することを特徴とする請求項 6 4 記載のドライブ装置。

8 6 . 前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

暗号化された暗号鍵を前記記録媒体から読出し、前記読み出され

た暗号鍵を前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて、復号された暗号鍵を再度暗号化したデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵で暗号化されたデータを前記記録媒体から読み出して復号することを特徴とする請求項 6 4 記載のドライブ装置。

8 7. 前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

鍵共有プロトコルによって共有した鍵を用いて暗号化した、データを暗号化する暗号鍵と前記暗号鍵を用いて暗号化したデータとを前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて再度暗号化した暗号鍵と、前記暗号鍵を用いて暗号化したデータとを前記記録媒体に記録することを特徴とする請求項 6 4 記載のドライブ装置。

8 8. 前記インターフェース部を介してデータを前記記録媒体に記録する処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記セキュリティーモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

鍵共有プロトコルによって共有した鍵を用いてデータを暗号化して前記セキュリティーモジュールに送り、

前記セキュリティーモジュールが、前記暗号化されたデータを共有された鍵を用いて復号し、暗号鍵を用いて、復号したデータを暗号化して記録媒体に格納することを特徴とする請求項 6 4 記載のドライブ装置。

8 9. 前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記セキュリティーモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティーモジュールが、暗号化された暗号鍵と前記暗号鍵を用いて暗号化されたデータとを前記記録媒体から読出し、前記暗号化された暗号鍵を前記セキュリティーモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて再度暗号化した暗号鍵と前記記録媒体から読み出した暗号鍵で暗号化されたデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティーモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵を用いて、暗号化されたデータを復号することを特徴と

する請求項 6 4 記載のドライブ装置。

9 0 . 前記インターフェース部を介して暗号化されたデータを前記記録媒体から読み出す処理を行う装置であり、

前記インターフェース部は、前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記セキュリティーモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティーモジュールが、暗号化されて情報記録媒体に格納されているデータを読み出すと共に、暗号鍵を用いて暗号化されたデータを復号し、前記鍵共有プロトコルによって共有した鍵を用いて、復号されたデータを再度暗号化したデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティーモジュールから受信した暗号化されたデータを復号することを特徴とする請求項 6 4 記載のドライブ装置。

9 1 . データを記録する記録媒体と、ドライブ装置との間で相互認証プロトコルを実行するセキュリティーモジュールとを具備する情報記録媒体に、アクセスするアクセス方法であって、

前記情報記録媒体へのアクセス時に相互認証プロトコルを実行し、

前記相互認証プロトコルの認証結果に応じて、前記情報記録媒体の記録媒体にアクセスすることを特徴とするアクセス方法。

9 2 . 前記相互認証プロトコルは、公開鍵暗号技術を用いたプロトコルであることを特徴とする請求項 9 1 記載のアクセス方法。

9 3 . 前記情報記録媒体の記録媒体であるメモリチップにアクセスすることを特徴とする請求項 9 1 記載のアクセス方法。

9 4 . 直接、前記記録媒体にアクセスすることを特徴とする請求項

9 1 記載のアクセス方法。

9 5 . 前記インターフェース部は、前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスすることを特徴とする請求項 9 1 記載のアクセス方法。

9 6 . 自己を識別する為の識別情報を記憶し、

前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持している当該情報記録媒体を識別するための識別情報と、自己が記憶している識別情報を交換し、前記セキュリティモジュールとの間で前記識別情報を交換し、互いに相手の識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 9 1 記載のアクセス方法。

9 7 . 前記セキュリティモジュールと自己の何れか一方若しくは両方がリストを保持するか否かに応じた相互認証プロトコルを実行することを特徴とする請求項 9 6 記載のアクセス方法。

9 8 . 前記セキュリティモジュールが前記リストを記憶している前記情報記録媒体か否かを判別し、その判別結果に基づいた相互認証プロトコルを実行することを特徴とする請求項 9 6 記載のアクセス方法。

9 9 . 前記リストのバージョン番号及びリストを記憶しており、

前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持するリストのバージョン番号と自己が記憶している前記リストのバージョン番号を交換し、自己が新しいリストを持つときそれをセキュリティモジュールに送り、自己が古いリストを持つときはセキュリティモジュールから送られた新しいリストを用いて自分の



リストを更新することを特徴とする請求項 9 6 記載のアクセス方法。

1 0 0 . 前記リストのバージョン番号及びリストを記憶し、

前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持するリストのバージョン番号と自己が記憶している前記リストのバージョン番号を交換し、自己のリストが新しい場合には、自己のリストを前記情報記録媒体の記録媒体上に書き込み、自己のリストが古い場合には、前記情報記録媒体の記録媒体上に記録されているリストを読み出し、読み出したリストを用いて自分のリストを更新することを特徴とする請求項 9 6 記載のアクセス方法。

1 0 1 . 前記セキュリティモジュールとの間で、共に上記新しいリストを用いて、相手の識別情報がリストに登録されているか否かを確認することを特徴とする請求項 9 6 記載のアクセス方法。

1 0 2 . 前記相互認証プロトコル処理時に、前記情報記録媒体がその内部に保持している当該情報記録媒体を識別するための識別情報を前記セキュリティモジュールから受信し、前記セキュリティモジュールの識別情報が不正な機器を排除するためのリストに登録されているか否かを確認し、排除すべき機器となっている場合には、相互認証プロトコルの以後のプロセスを行わないことを特徴とする請求項 9 1 記載のアクセス方法。

1 0 3 . 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたリストであり、このリストに登録されている機器を排除すべき機器とすることを特徴とする請求項 9 6 又は請求項 1 0 2 記載のアクセス方法。

1 0 4 . 前記不正な機器を排除するためのリストは、排除すべきでない機器の識別情報が登録されたリストであり、このリストに登録

されていない機器を排除すべき機器とする請求項 9 6 又は請求項 1 0 2 記載のアクセス方法。

1 0 5 . 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、リボケーションリストに登録されている、及び／又は、レジストレーションリストに登録されていない機器を排除すべき機器とすることを特徴とする請求項 9 6 又は請求項 1 0 2 記載のアクセス方法。

1 0 6 . 前記不正な機器を排除するためのリストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されており、前記リボケーションリストとレジストレーションリストのうち何れか一方を選択的に、排除すべき機器となっているか否かを判定することを特徴とする請求項 9 6 又は請求項 1 0 2 記載のアクセス方法。

1 0 7 . 前記相互認証プロトコルを実行時に、自己と前記セキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を暗号化して一方から他方に送ることを特徴とする請求項 9 1 記載のアクセス方法。

1 0 8 . 前記相互認証プロトコルを実行時に、自己とセキュリティモジュールとが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化して一方から他方に送ることを特徴とする請求項 9 1 記載のアクセス方法。

1 0 9 . 前記セキュリティモジュールとの間で公開鍵暗号を用いて

鍵共有プロトコルを実行し、

前記鍵共有プロトコルによって共有した鍵を用いて、データを暗号化する暗号鍵を暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いて復号された暗号鍵を再度暗号化したデータを受信し、

前記暗号鍵で暗号化されたデータと前記セキュリティモジュールによって保存鍵で暗号化された暗号鍵を記録媒体に記録することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 0. 前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

暗号化された暗号鍵を前記記録媒体から読出し、前記読み出された暗号鍵を前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて、復号された暗号鍵を再度暗号化したデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵で暗号化されたデータを前記記録媒体から読み出して復号することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 1. 前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有

プロトコルを実行し、

鍵共有プロトコルによって共有した鍵を用いて暗号化した、データを暗号化する暗号鍵と前記暗号鍵を用いて暗号化したデータとを前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化された暗号鍵を鍵共有プロトコルによって共有された鍵を用いて復号し、前記セキュリティモジュールに記憶された保存鍵を用いてを再度暗号化した暗号鍵と、前記暗号鍵を用いて暗号化したデータとを前記記録媒体に記録することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 2. 前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

鍵共有プロトコルによって共有した鍵を用いてデータを暗号化して前記セキュリティモジュールに送り、

前記セキュリティモジュールが、前記暗号化されたデータを共有された鍵を用いて復号し、暗号鍵を用いて、復号したデータを暗号化して記録媒体に格納することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 3. 前記情報記録媒体のセキュリティーモジュールを介して記録媒体にアクセスし、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールが、暗号化された暗号鍵と前記暗号鍵を用いて暗号化されたデータとを前記記録媒体から読出し、前記

暗号化された暗号鍵を前記セキュリティモジュールに記憶された保存鍵を用いて復号し、鍵共有プロトコルによって共有された鍵を用いて再度暗号化した暗号鍵と前記記録媒体から読み出した暗号鍵で暗号化されたデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化された暗号鍵を復号し、前記暗号鍵を用いて、暗号化されたデータを復号することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 4 . 前記情報記録媒体のセキュリティモジュールを介して記録媒体にアクセスし、

前記セキュリティモジュールとの間で公開鍵暗号を用いて鍵共有プロトコルを実行し、

前記セキュリティモジュールが、暗号化されて情報記録媒体に格納されているデータを読み出すと共に、暗号鍵を用いて暗号化されたデータを復号し、前記鍵共有プロトコルによって共有した鍵を用いて、復号されたデータを再度暗号化したデータを受信し、

前記鍵共有プロトコルによって共有された鍵を用いて、前記セキュリティモジュールから受信した暗号化されたデータを復号することを特徴とする請求項 9 1 記載のアクセス方法。

1 1 5 . データを記録する記録領域を有する情報記録媒体において、

外部装置とインターフェースをとるためのインターフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールと、

データを記録する前記記録領域を有する記録媒体とを具備するこ

とを特徴とする情報記録媒体。

116. 上記セキュリティモジュールは、データを記録する前記記録媒体にアクセスするためのインターフェース機能を更に具備することを特徴とする請求項115記載の情報記録媒体。

117. データを記録する記録領域を有する情報記録媒体のアクセス方法において、

外部装置と接続し、

乱数を生成して前記外部装置に送信し、

前記外部装置から受信した情報と、保存している情報とを使用して、前記外部装置との間で公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行い、

前記外部装置との間で相互認証プロトコルを実行し、

前記相互認証プロトコルの認証結果に応じて、前記記録領域にアクセスすることを特徴とするアクセス方法。

118. 情報記録媒体を製造する記録媒体製造装置であって、

記録媒体にアクセスするドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、データを記録する記録媒体とを具備する情報記録媒体に、不正な機器を排除する処理に用いられるリストを記録する記録部を具備することを特徴とする記録媒体製造装置。

119. 前記セキュリティモジュールと前記記録媒体とを有する前記情報記録媒体を組み立てる組立部を更に具備することを特徴とする請求項118記載の記録媒体製造装置。

120. 前記記録部は、前記セキュリティモジュール内に前記リストを記録することを特徴とする請求項118記載の記録媒体製造装

置。

1 2 1. 前記記録部は、前記リストのバージョン番号及び前記リストを前記セキュリティーモジュール内に記録することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 2. 前記記録部は、前記記録媒体上に前記リストを記録することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 3. 前記記録部は、前記リストのバージョン番号を前記セキュリティーモジュール内に記録し、前記リストを前記記録媒体上に記録することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 4. 前記記録部は、前記情報記録媒体の識別情報、前記情報記録媒体に与えられた公開鍵暗号技術で用いられるプライベート鍵及びパブリック鍵証明書、前記リストのバージョン番号を前記セキュリティーモジュール内に記録することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 5. 前記記録部が前記情報記録媒体に記録する前記リストを格納する格納手段を更に具備することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 6. 前記記録部が前記情報記録媒体に記録する前記リストを外部から入手するインターフェースを更に具備することを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 7. 前記リストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び／又は排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されていることを特徴とする請求項 1 1 8 記載の記録媒体製造装置。

1 2 8. 情報記録媒体を製造する記録媒体製造方法であって、

記録媒体にアクセスするドライブ装置との間で相互認証プロトコルを実行するセキュリティモジュールと、データを記録する記録媒体とを具備する情報記録媒体に、不正な機器を排除する処理に用いられるリストを記録することを特徴とする記録媒体製造方法。

129. 前記セキュリティモジュールと前記記録媒体とを有する前記情報記録媒体を組み立てることを特徴とする請求項128記載の記録媒体製造方法。

130. 前記セキュリティモジュール内に前記リストを記録することを特徴とする請求項128記載の記録媒体製造方法。

131. 前記リストのバージョン番号及び前記リストを前記セキュリティモジュール内に記録することを特徴とする請求項128記載の記録媒体製造方法。

132. 前記記録媒体上に前記リストを記録することを特徴とする請求項128記載の記録媒体製造方法。

133. 前記リストのバージョン番号を前記セキュリティモジュール内に記録し、前記リストを前記記録媒体上に記録することを特徴とする請求項128記載の記録媒体製造方法。

134. 前記情報記録媒体の識別情報、前記情報記録媒体に与えられた公開鍵暗号技術で用いられるプライベート鍵及びパブリック鍵証明書、前記リストのバージョン番号を前記セキュリティモジュール内に記録することを特徴とする請求項128記載の記録媒体製造方法。

135. 前記情報記録媒体に記録する前記リストを格納することを特徴とする請求項128記載の記録媒体製造方法。

136. 前記情報記録媒体に記録する前記リストを外部から入手す

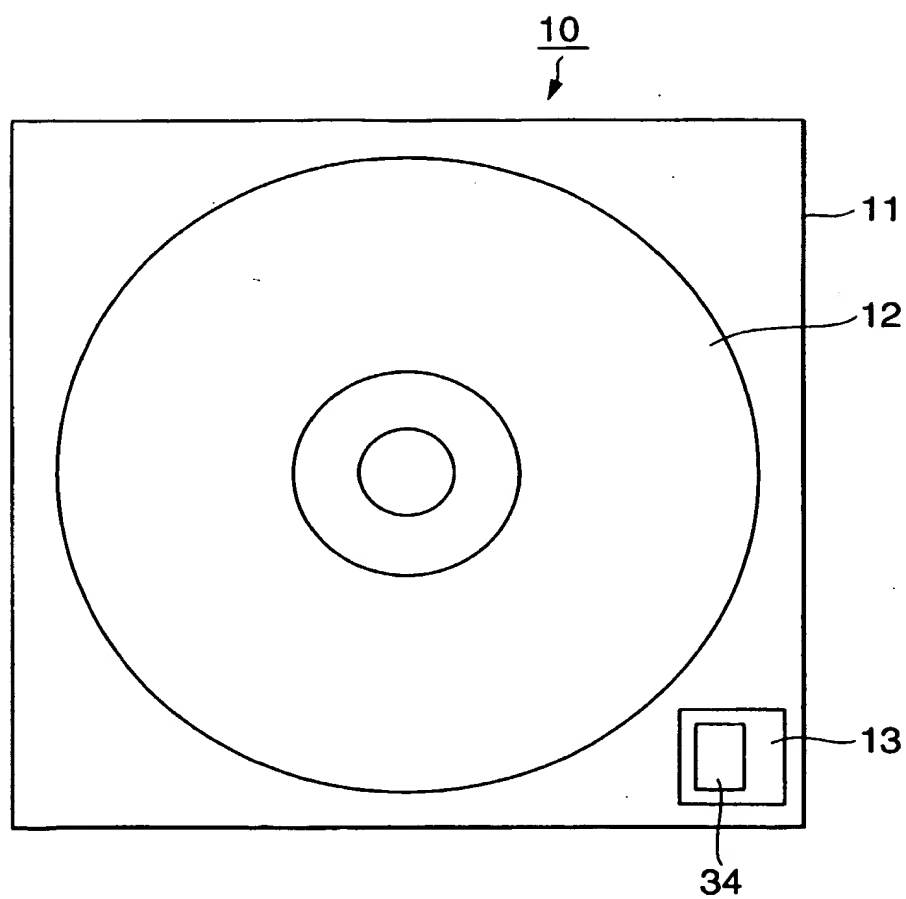


ることを特徴とする請求項 1 2 8 記載の記録媒体製造方法。

1 3 7. 前記リストは、排除すべき機器の識別情報が登録されたりボケーションリスト及び／又は排除すべきでない機器の識別情報が登録されたレジストレーションリストから構成されていることを特徴とする請求項 1 2 8 記載の記録媒体製造方法。

**THIS PAGE BLANK (USPTO)**

1/94

**FIG.1**

**THIS PAGE BLANK (USPTO)**

2/94

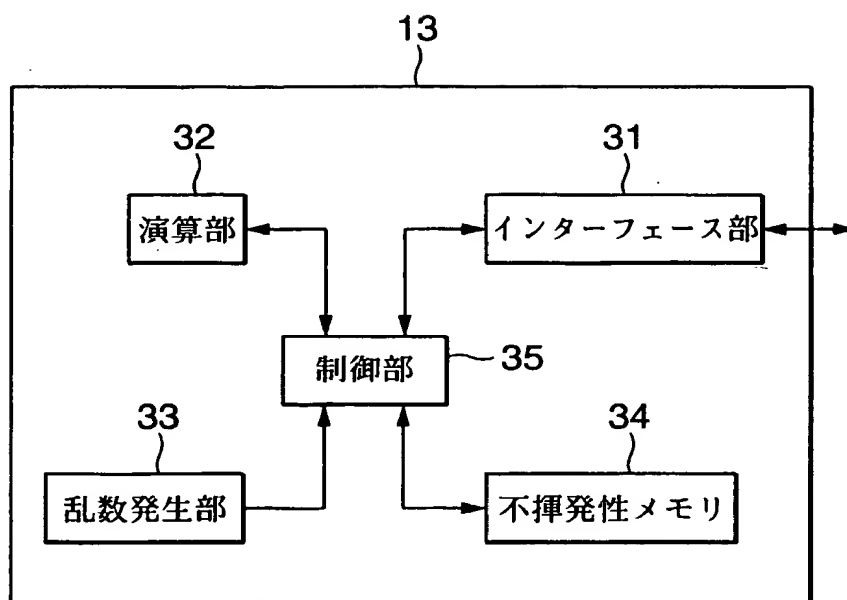


FIG.2

**THIS PAGE BLANK (USPTO)**

3/94

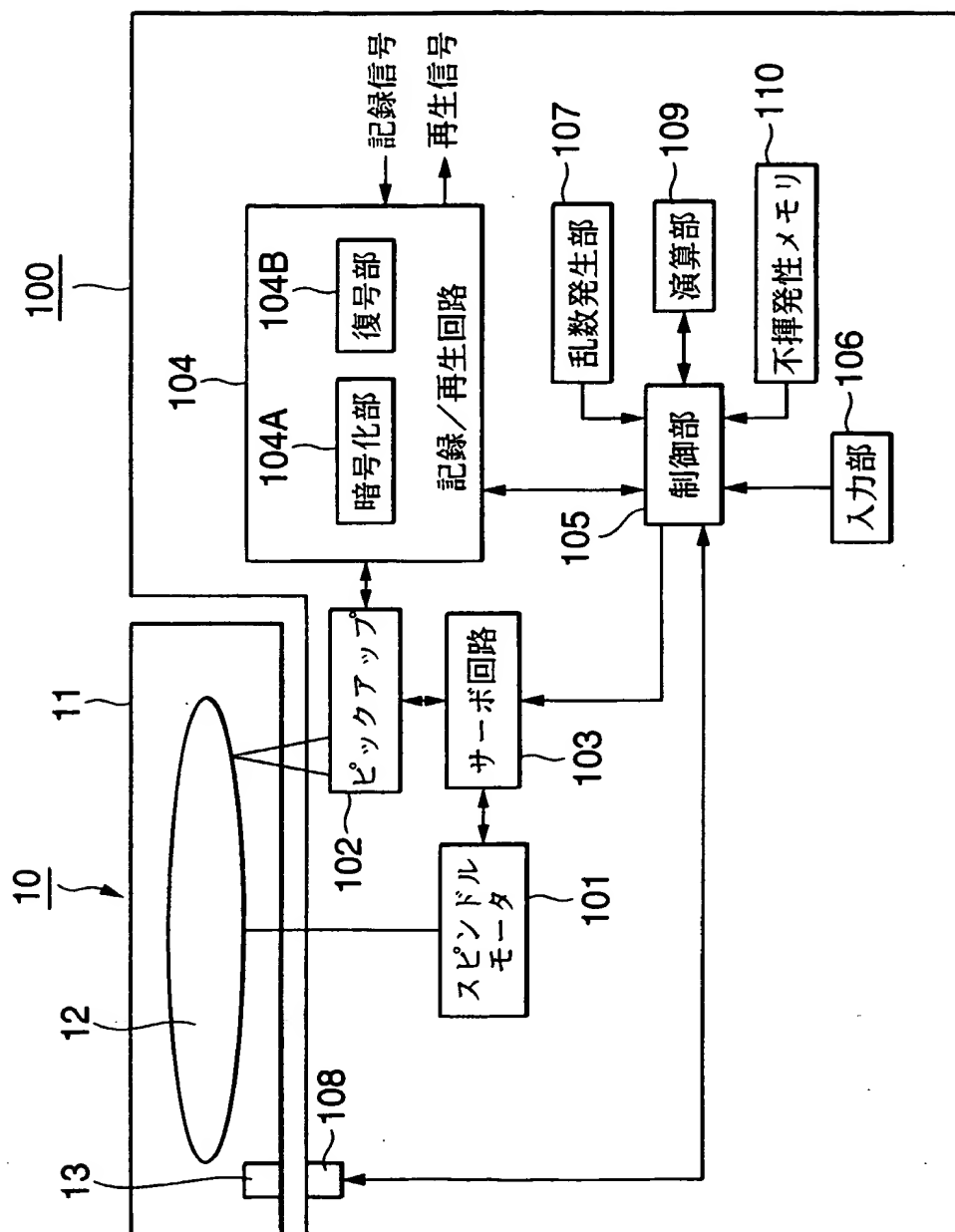


FIG.3

**THIS PAGE BLANK (USPTO)**



4/94

エンティティID
エンティティタイプ
エンティティ公開鍵
TCのデジタル署名

FIG.4

バージョンナンバー
リボークされる機器または媒体のID
.....
TCのデジタル署名

FIG.5

THIS PAGE BLANK (USPTO)

5/94

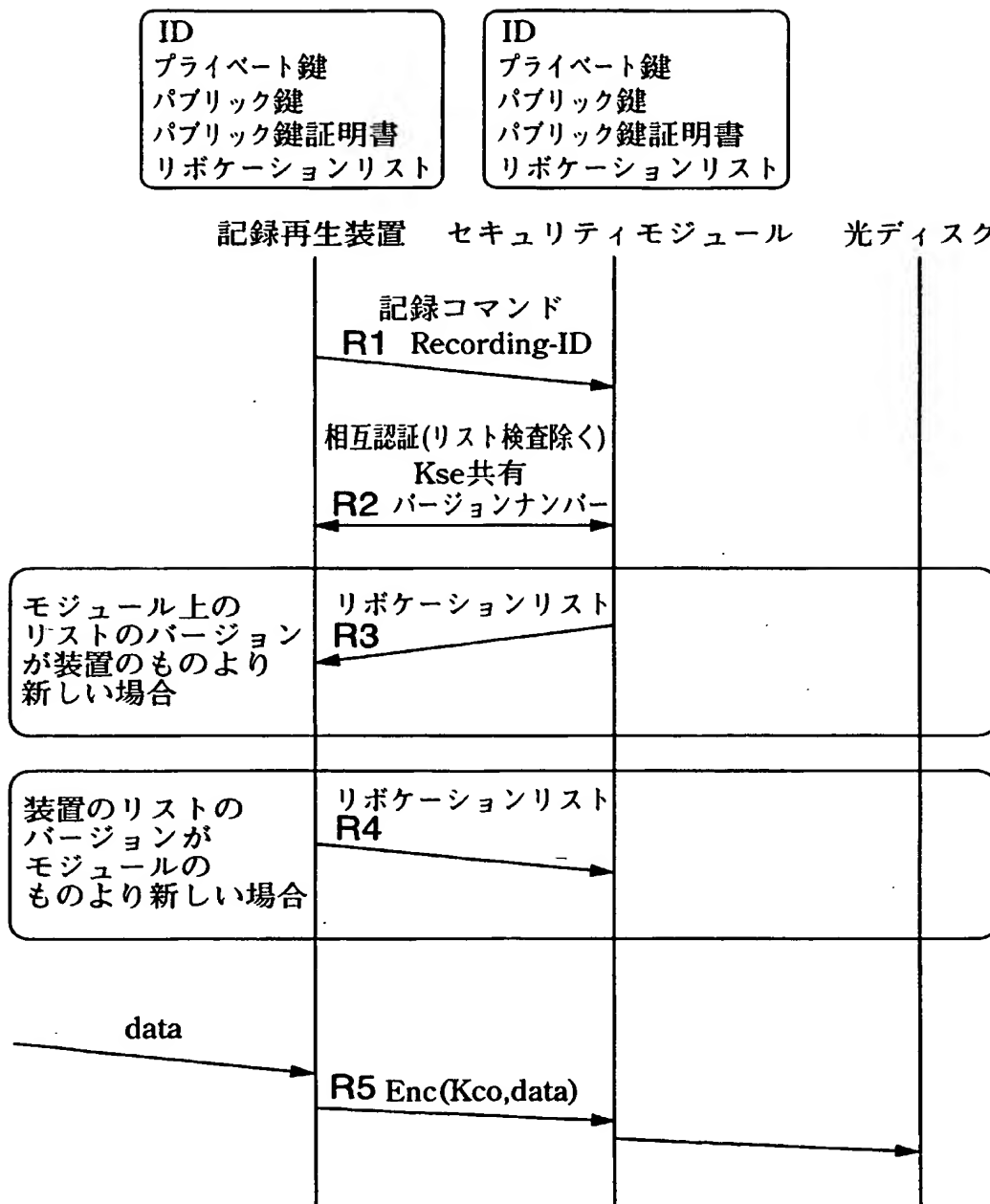


FIG.6

**THIS PAGE BLANK (USPTO)**

6/94

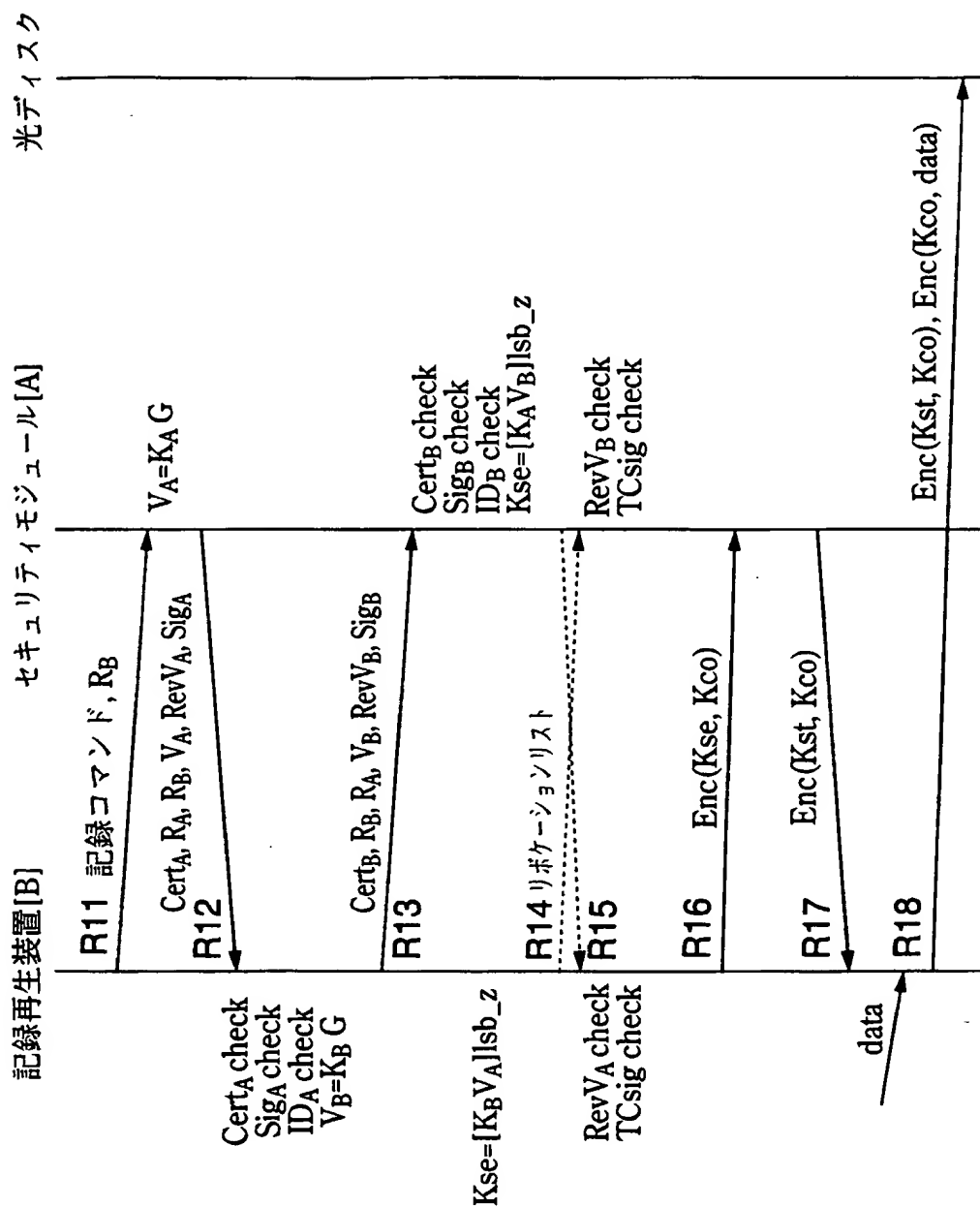


FIG.7

**THIS PAGE BLANK (USPTO)**

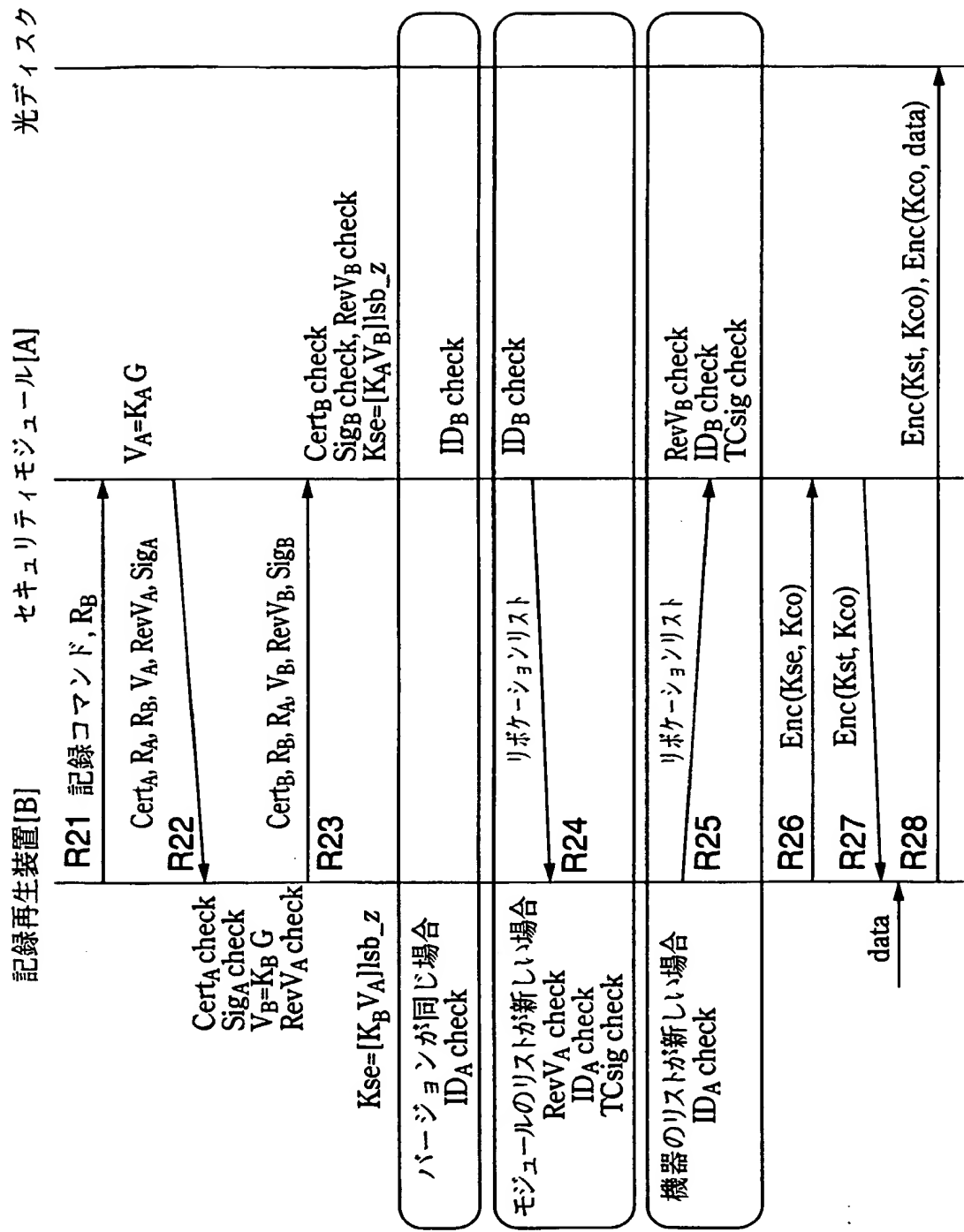


FIG.8

**THIS PAGE BLANK (USPTO)**



8/94

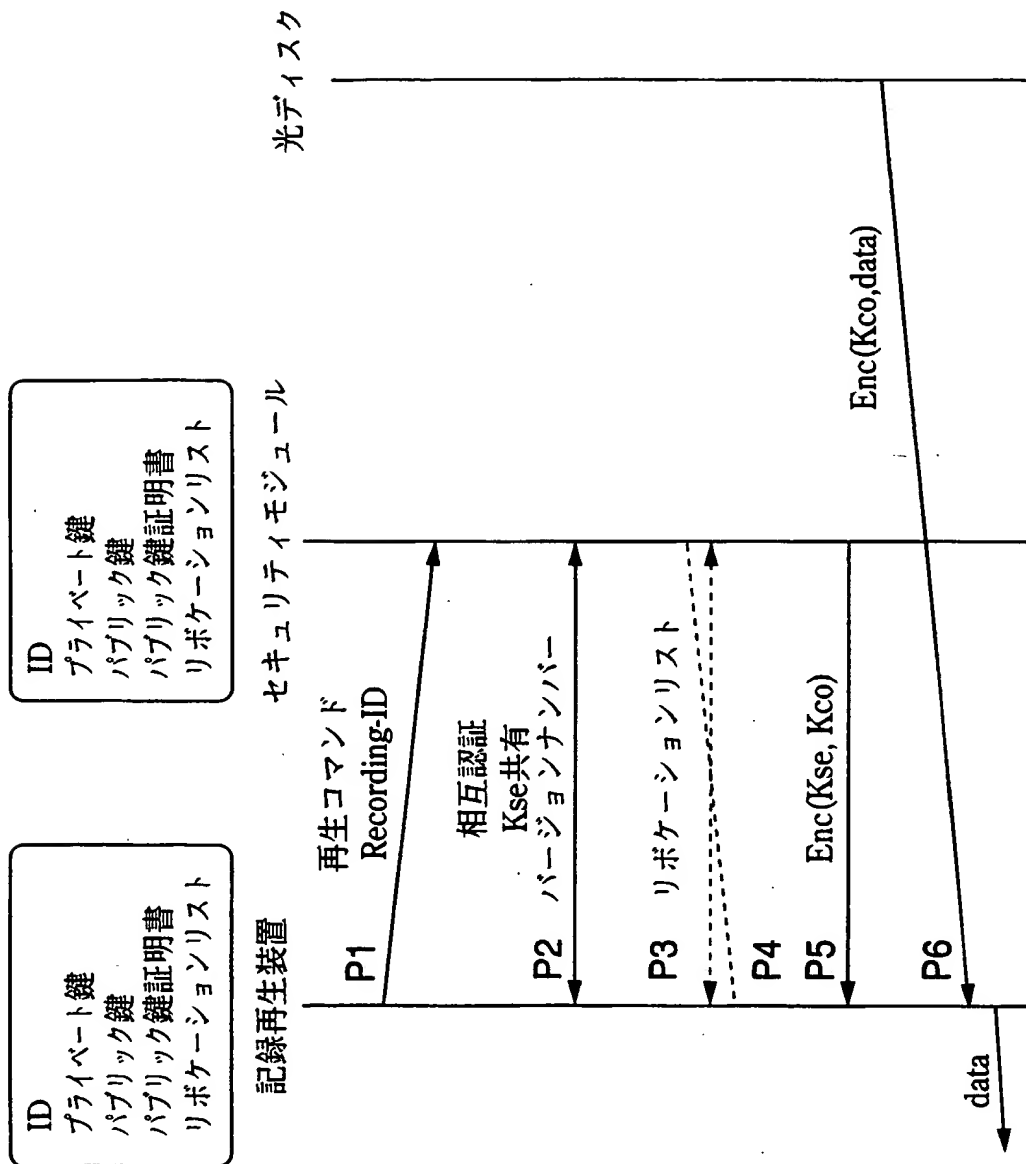


FIG.9

**THIS PAGE BLANK (USPTO)**

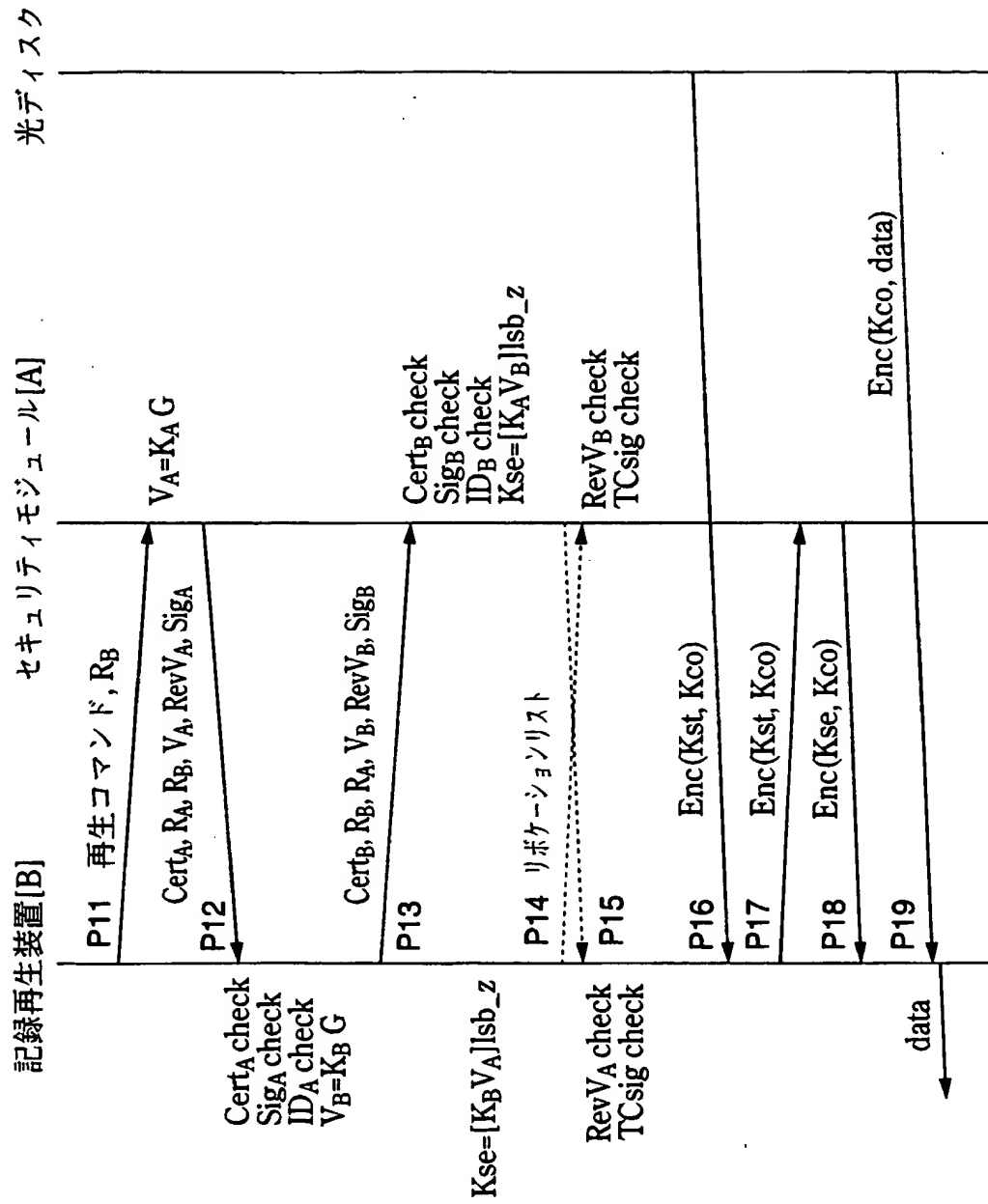


FIG.10

**THIS PAGE BLANK (USP 10)**

10/94

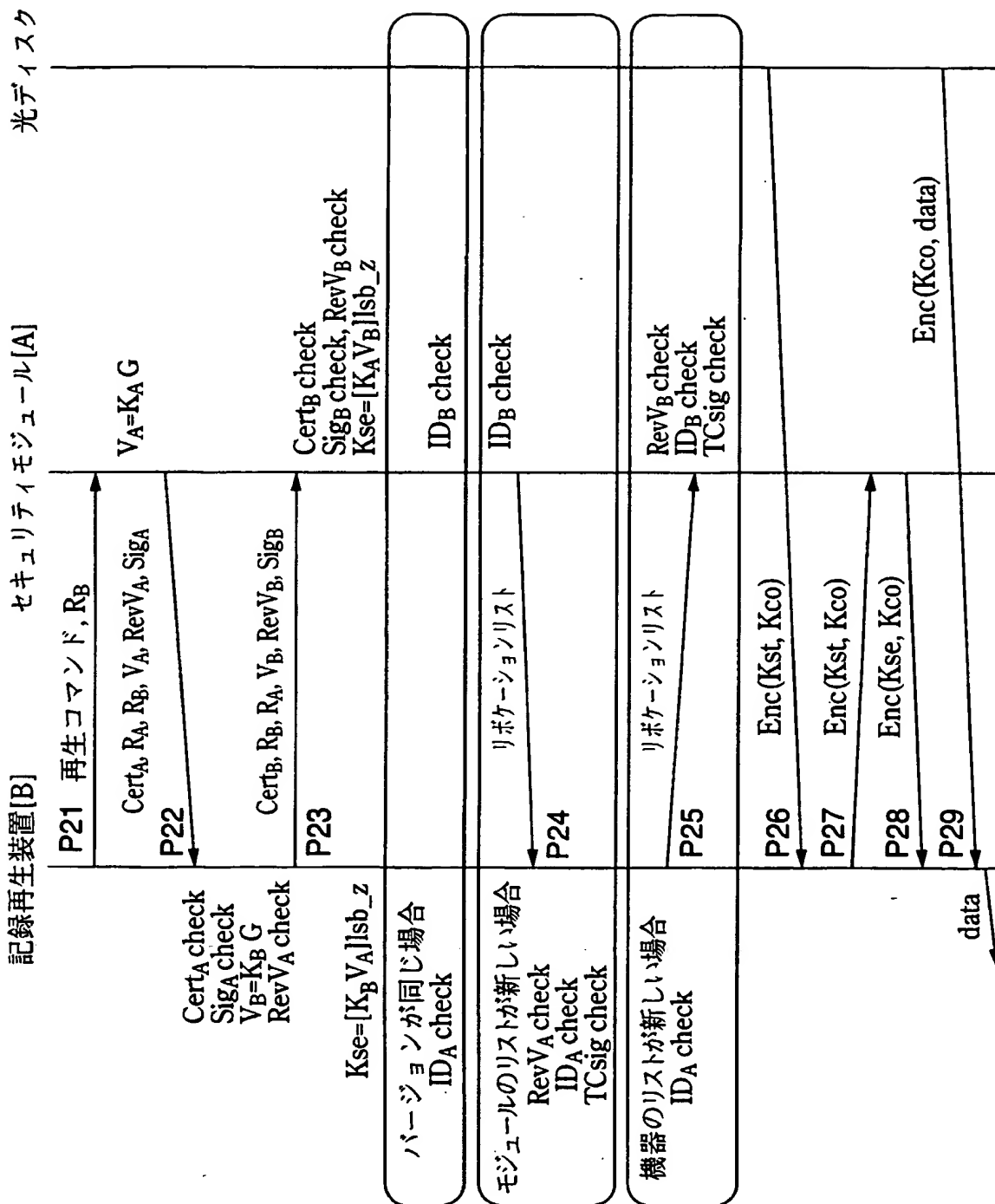


FIG.11

**THIS PAGE BLANK (USPTO)**

11/94

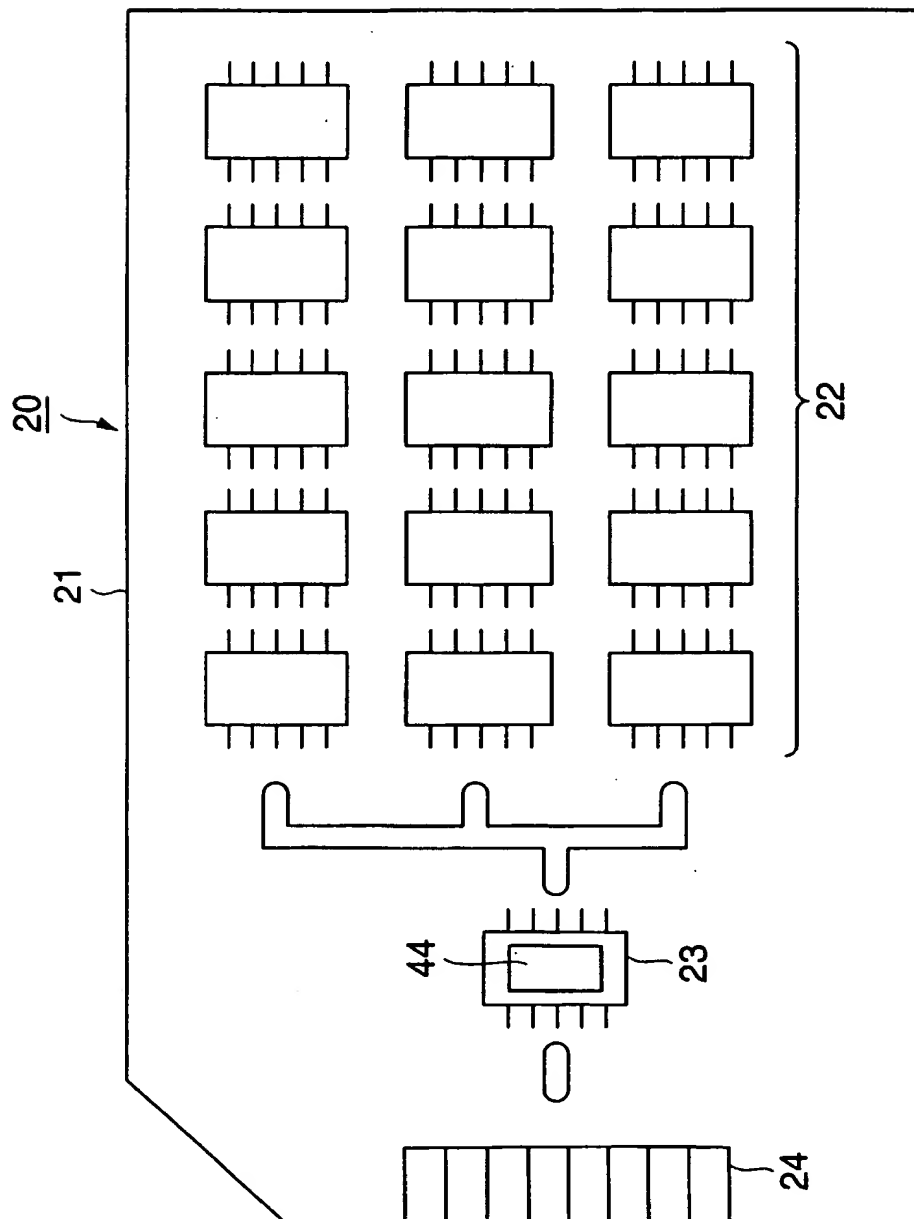


FIG.12

**THIS PAGE BLANK (USPTO)**



12/94

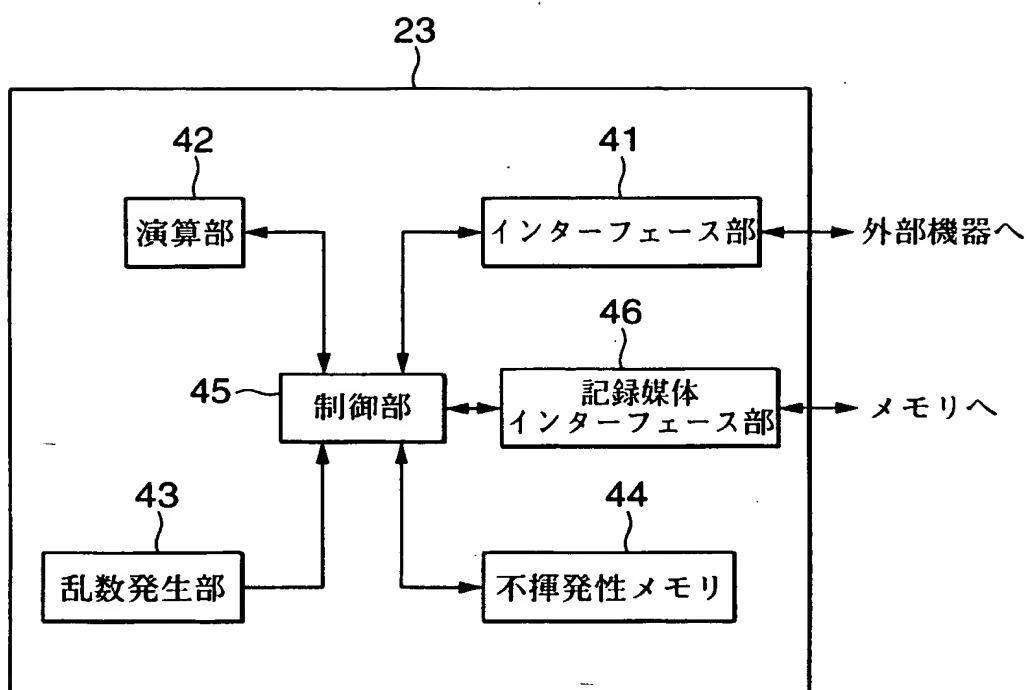


FIG.13

**THIS PAGE BLANK (USPTO)**

13/94

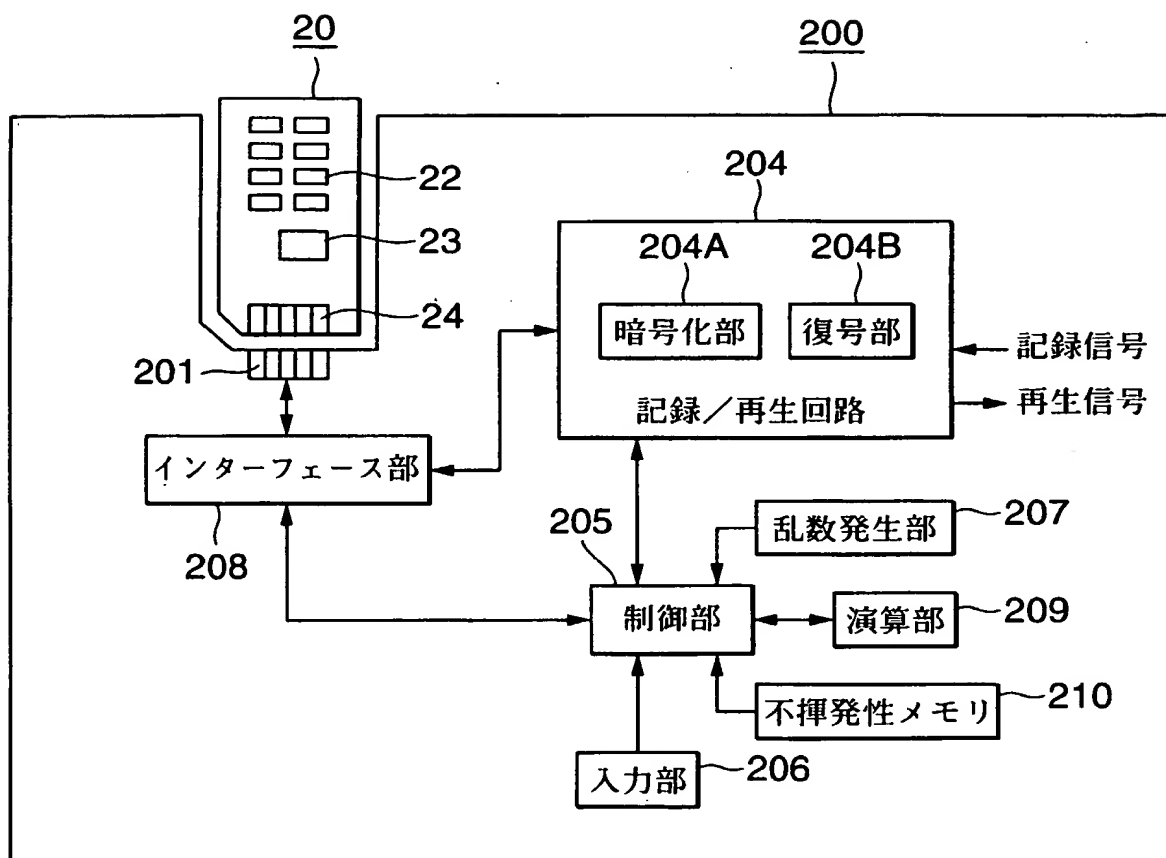


FIG.14

THIS PAGE BLANK (USPT)

14/94

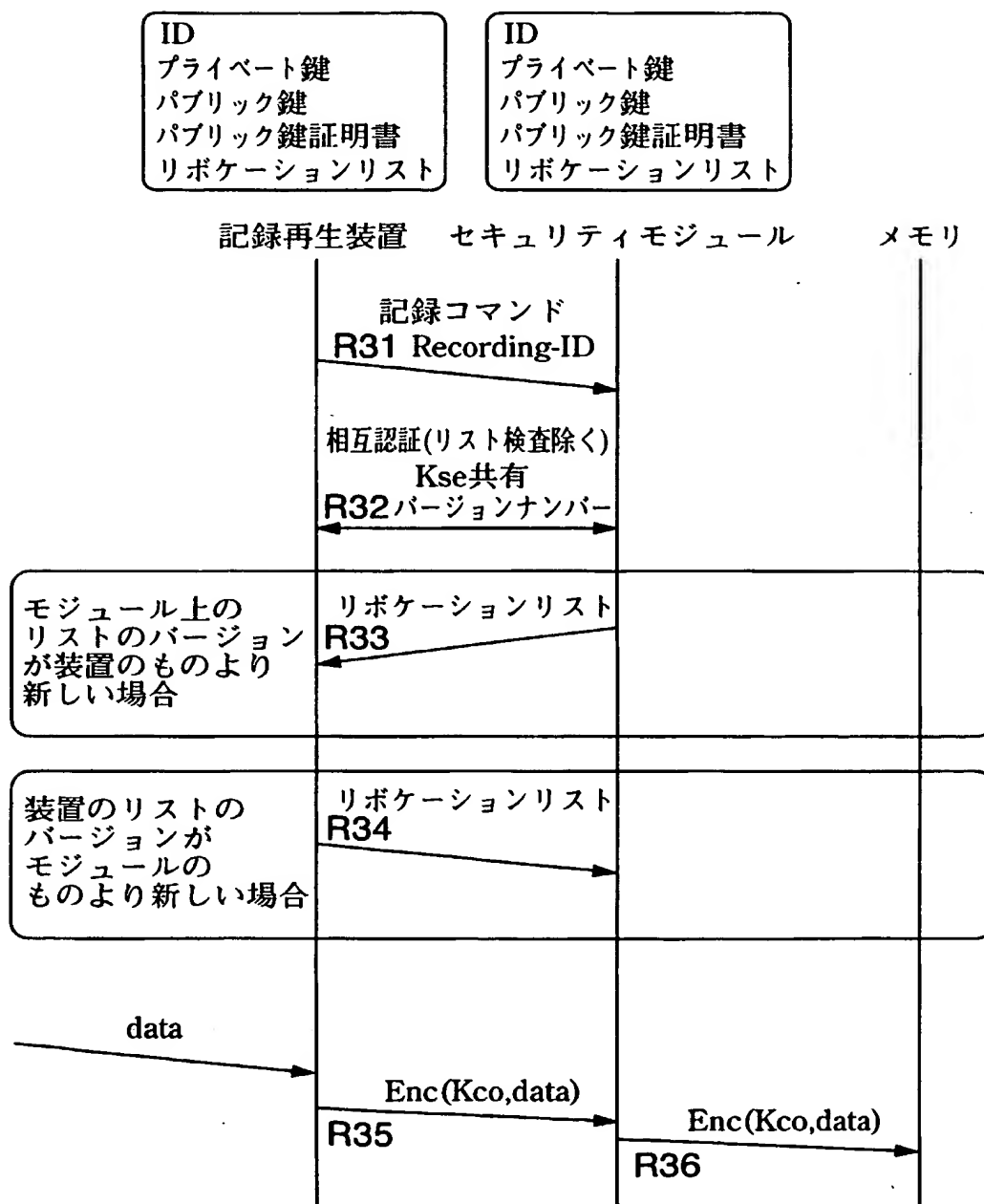


FIG.15

THIS PAGE BLANK

15/94

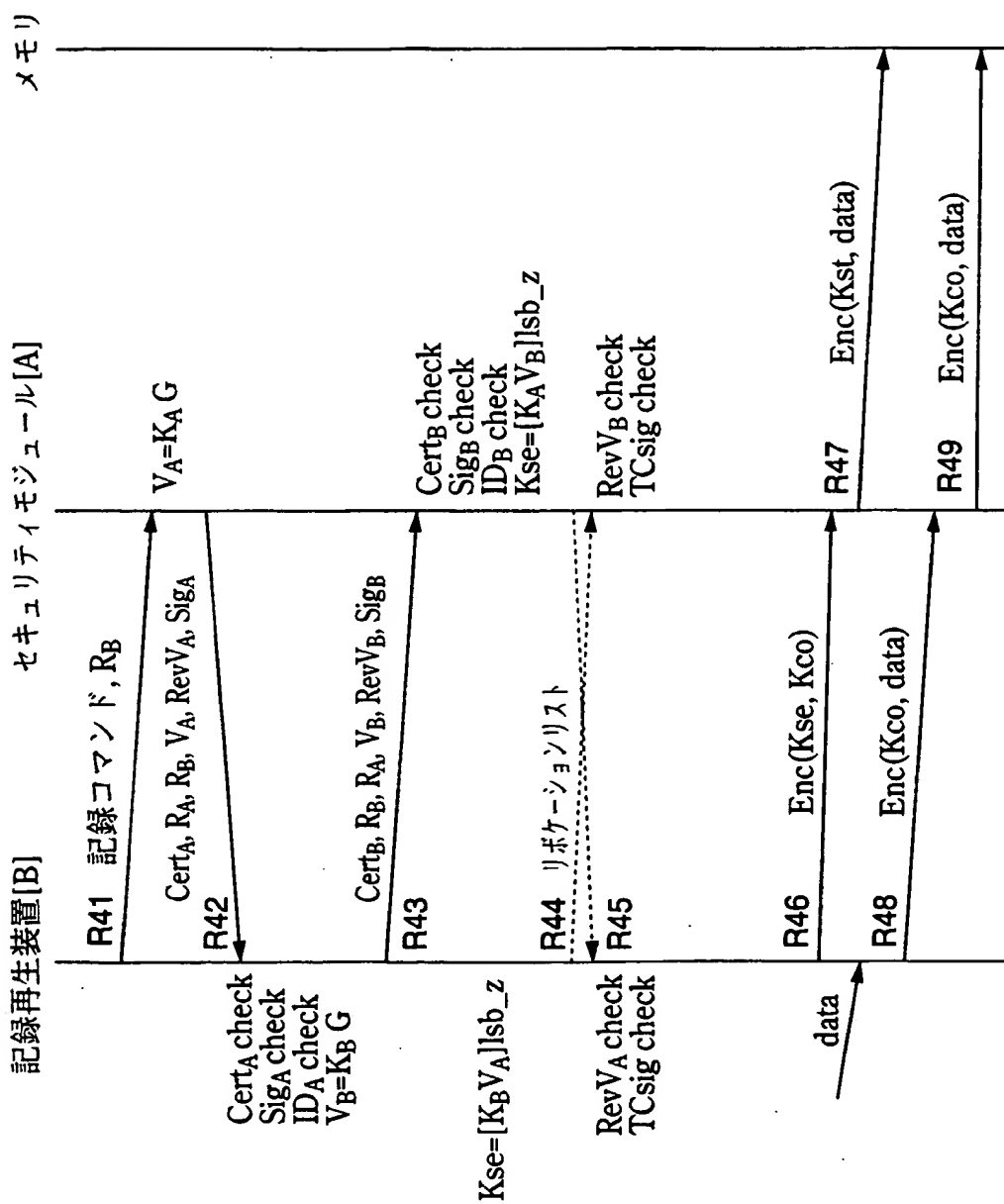


FIG.16

**THIS PAGE BLANK (USPTO)**



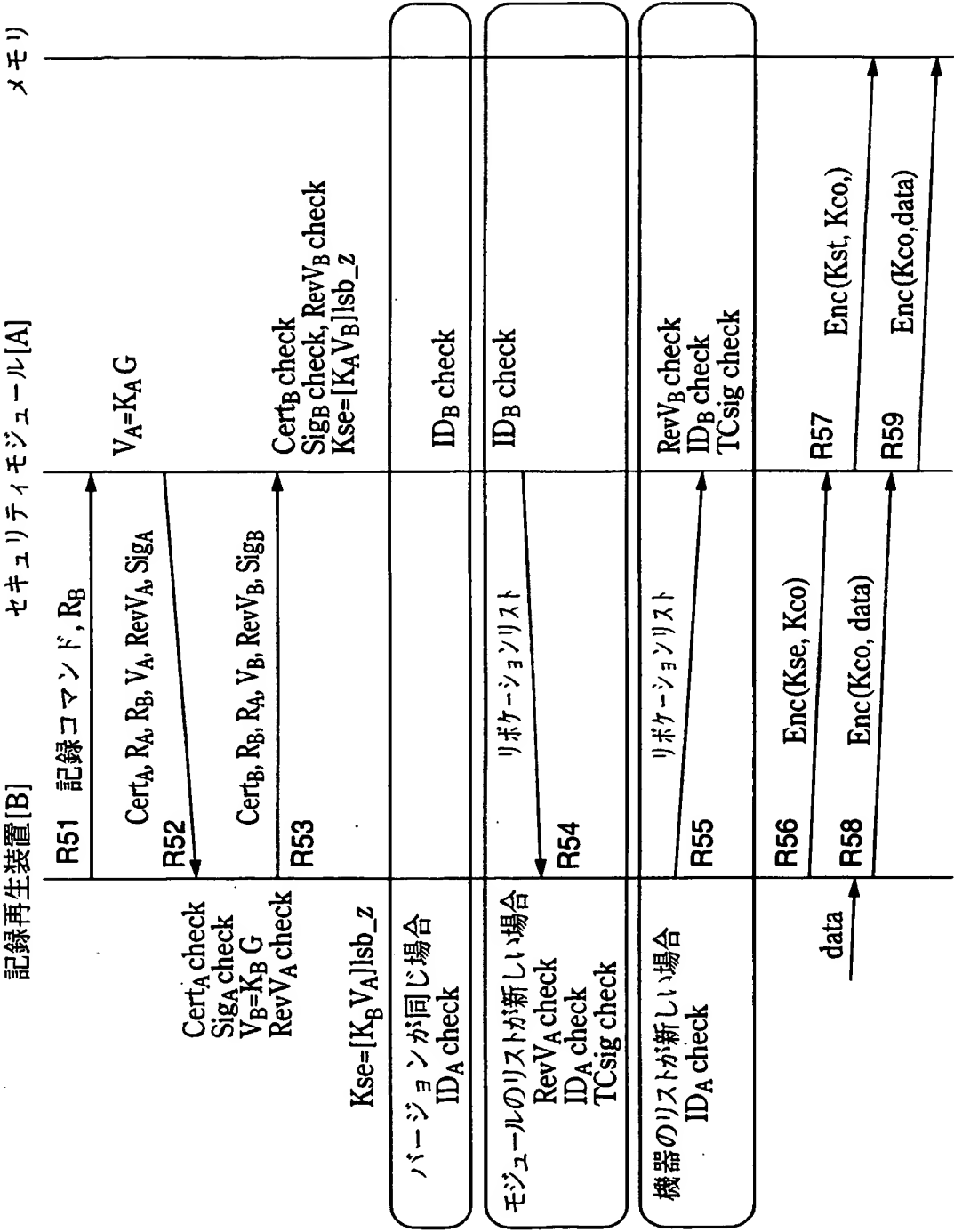


FIG.17

THIS PAGE BLANK (USPTO)

17/94

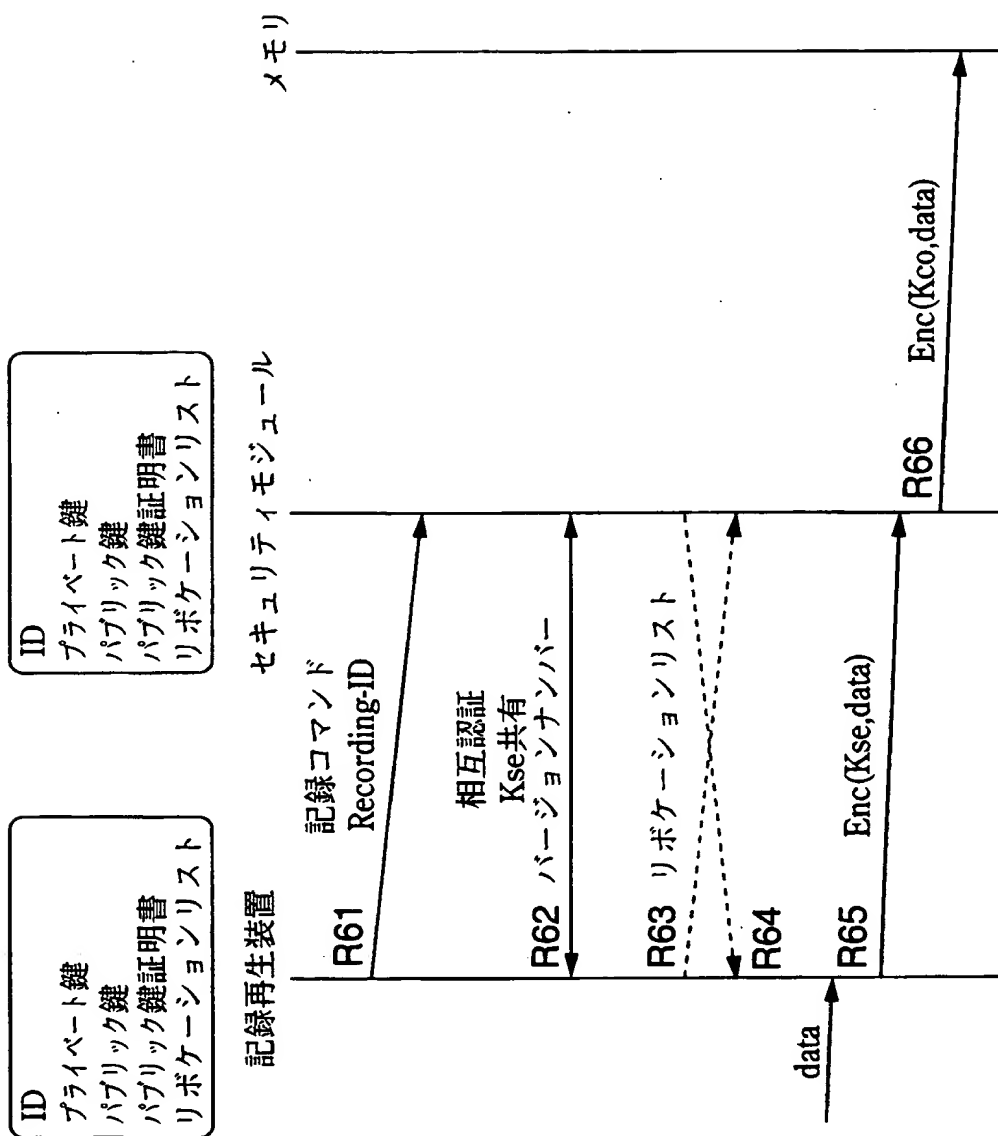


FIG.18

THIS PAGE BLANK

18/94

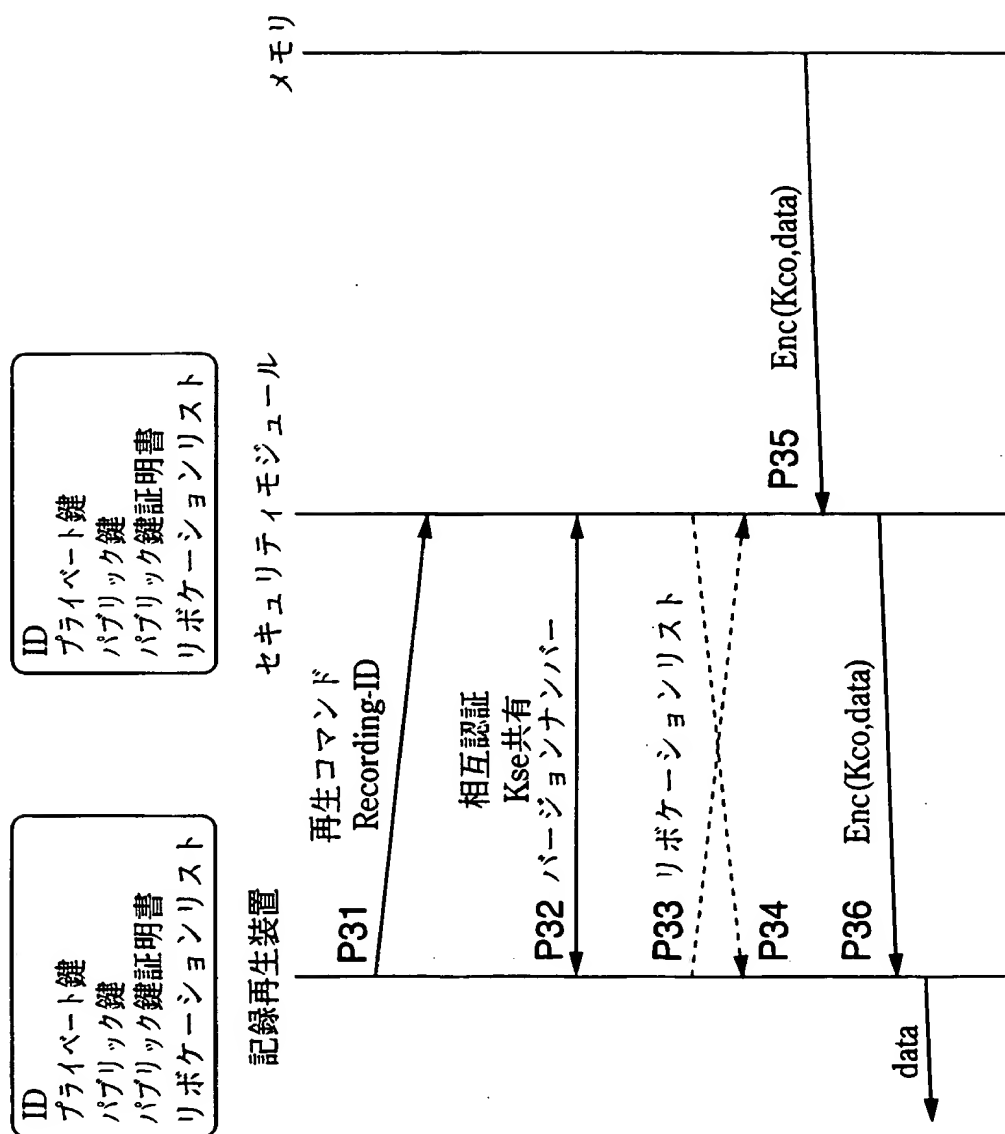


FIG.19

THIS PAGE BLANK (USPTO)

19/94

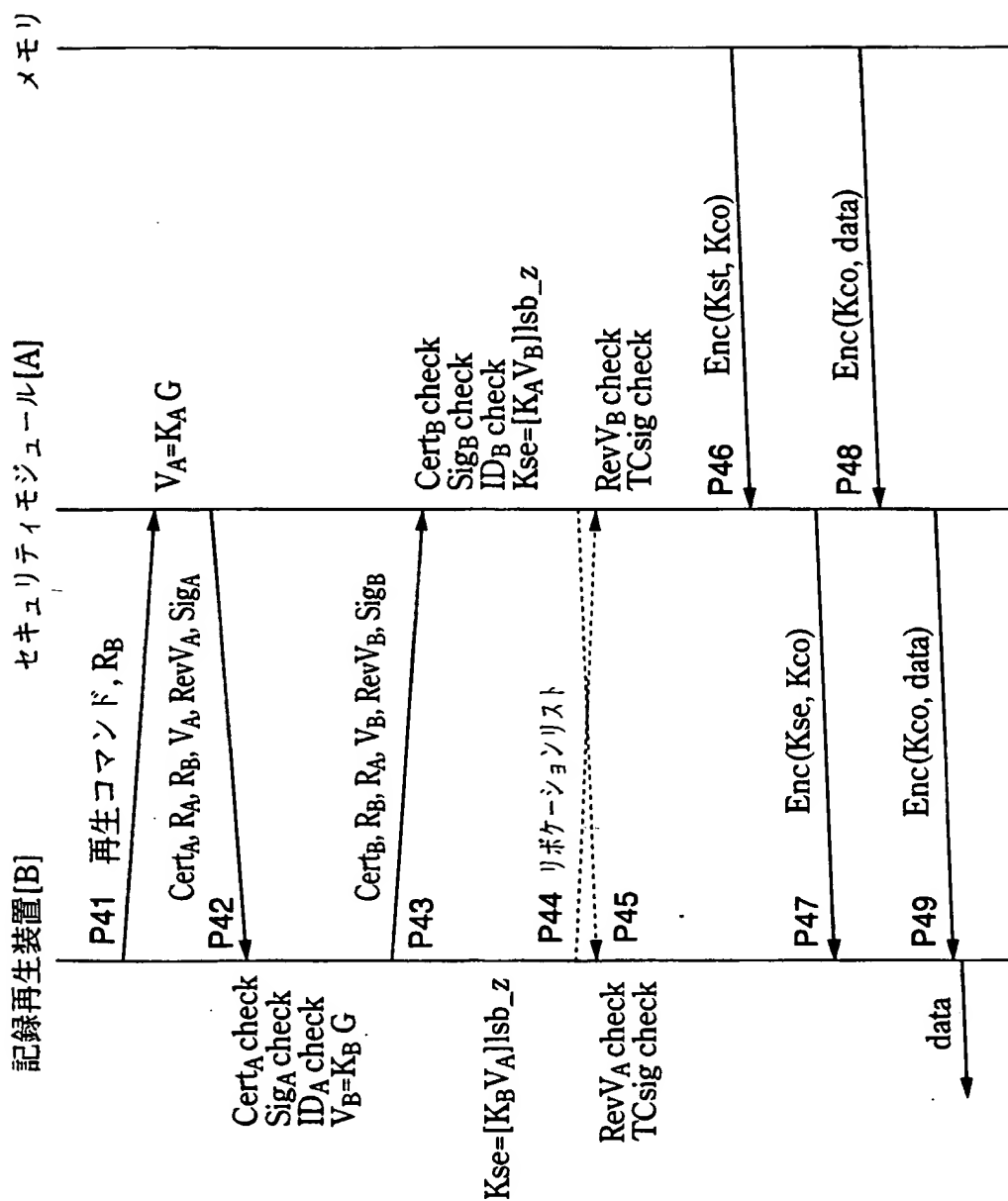


FIG.20

**THIS PAGE BLANK (USPTO)**



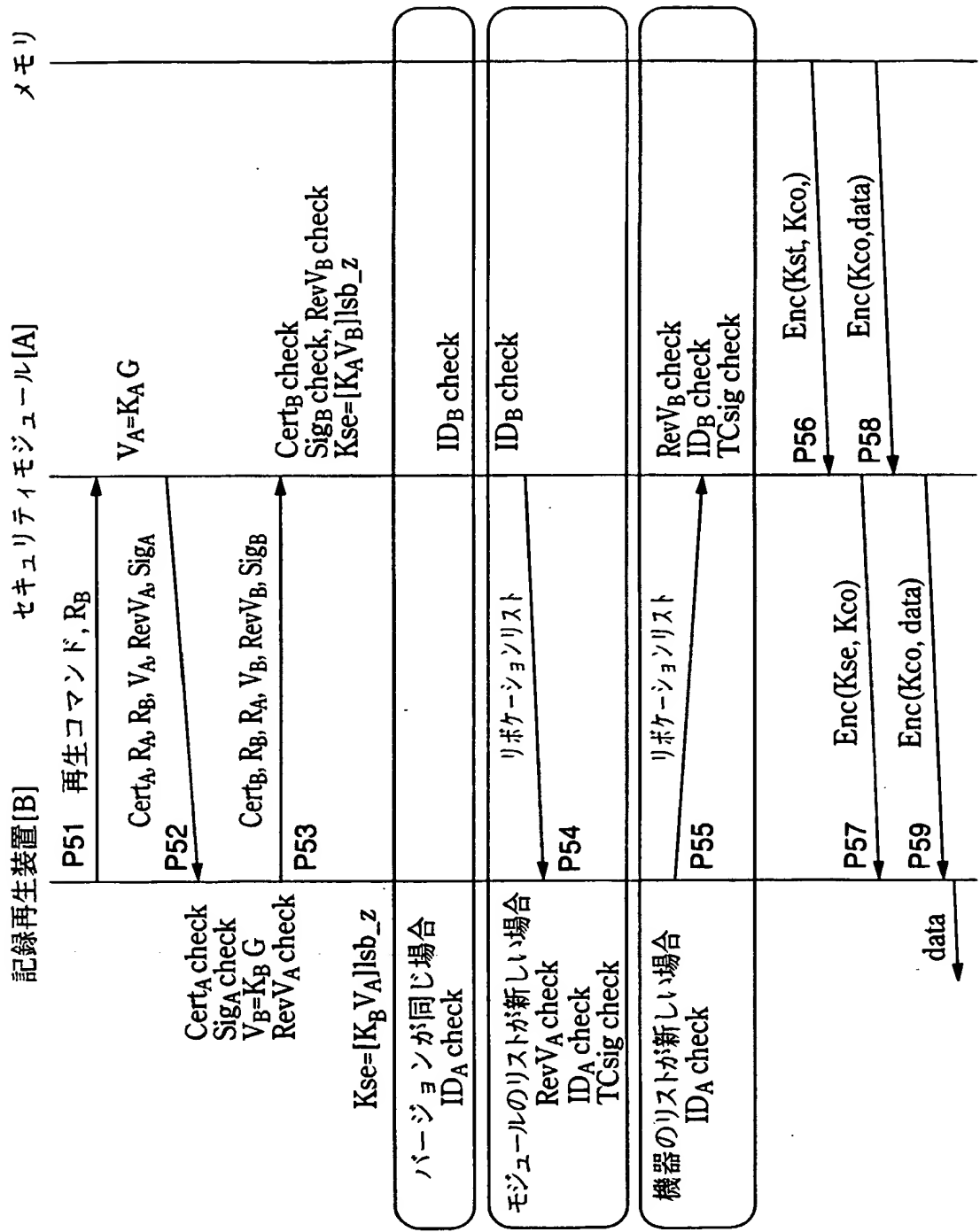


FIG.21

**THIS PAGE BLANK (USPTO)**

21/94

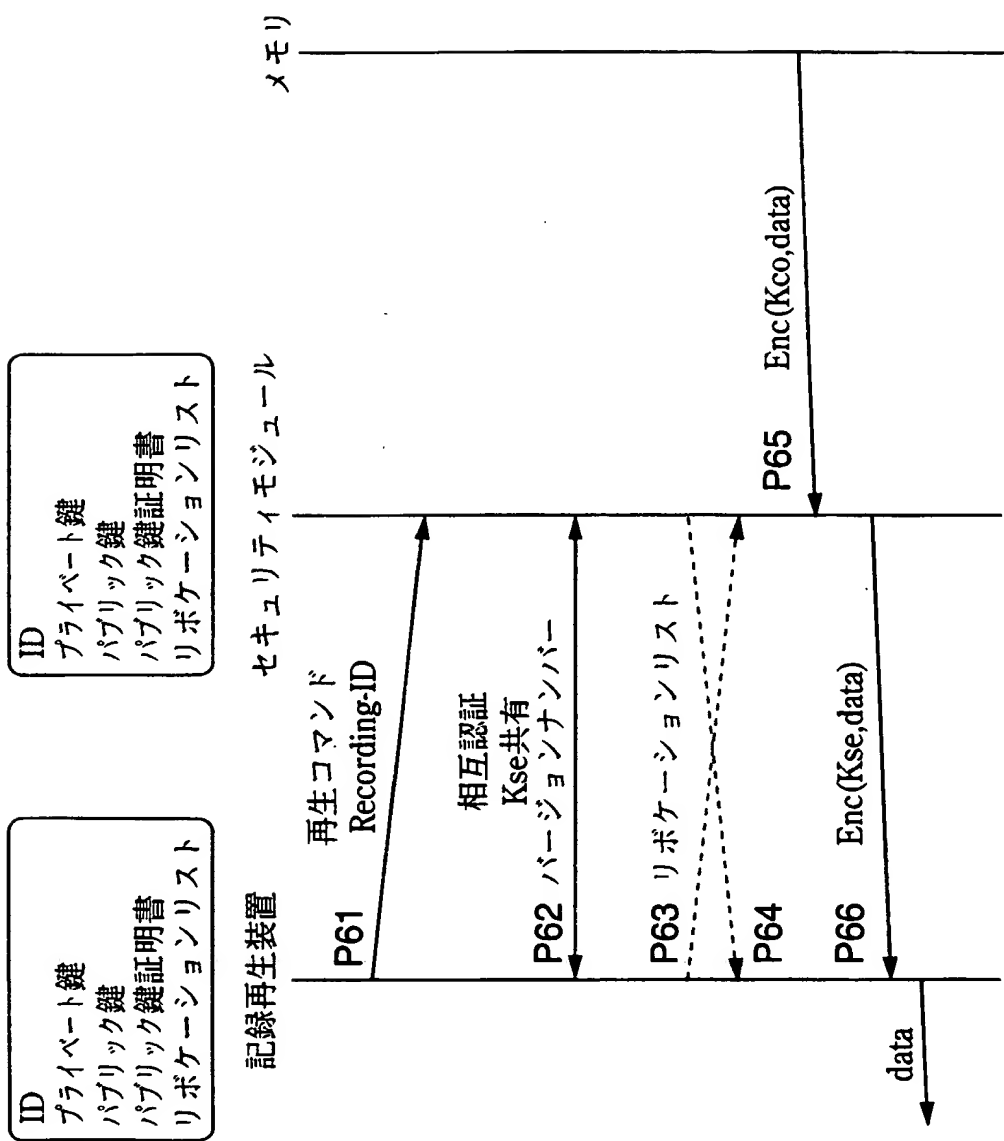


FIG.22

**THIS PAGE BLANK (USPTO)**

22/94

バージョンナンバー
登録される機器または媒体のID
.....
TCのデジタル署名

FIG.23

**THIS PAGE BLANK (USPTO)**

23/94

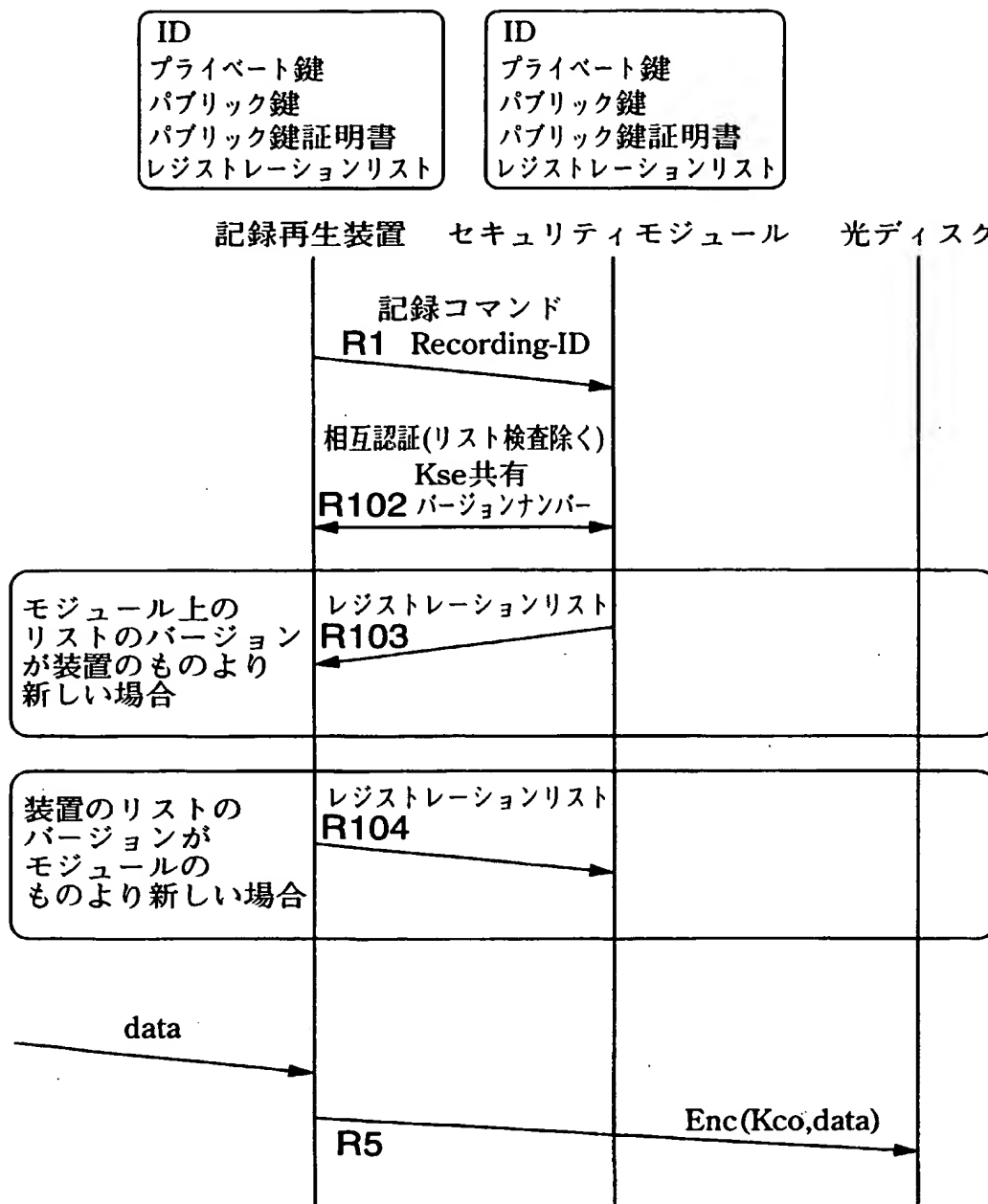


FIG.24

**THIS PAGE BLANK (OSP)**



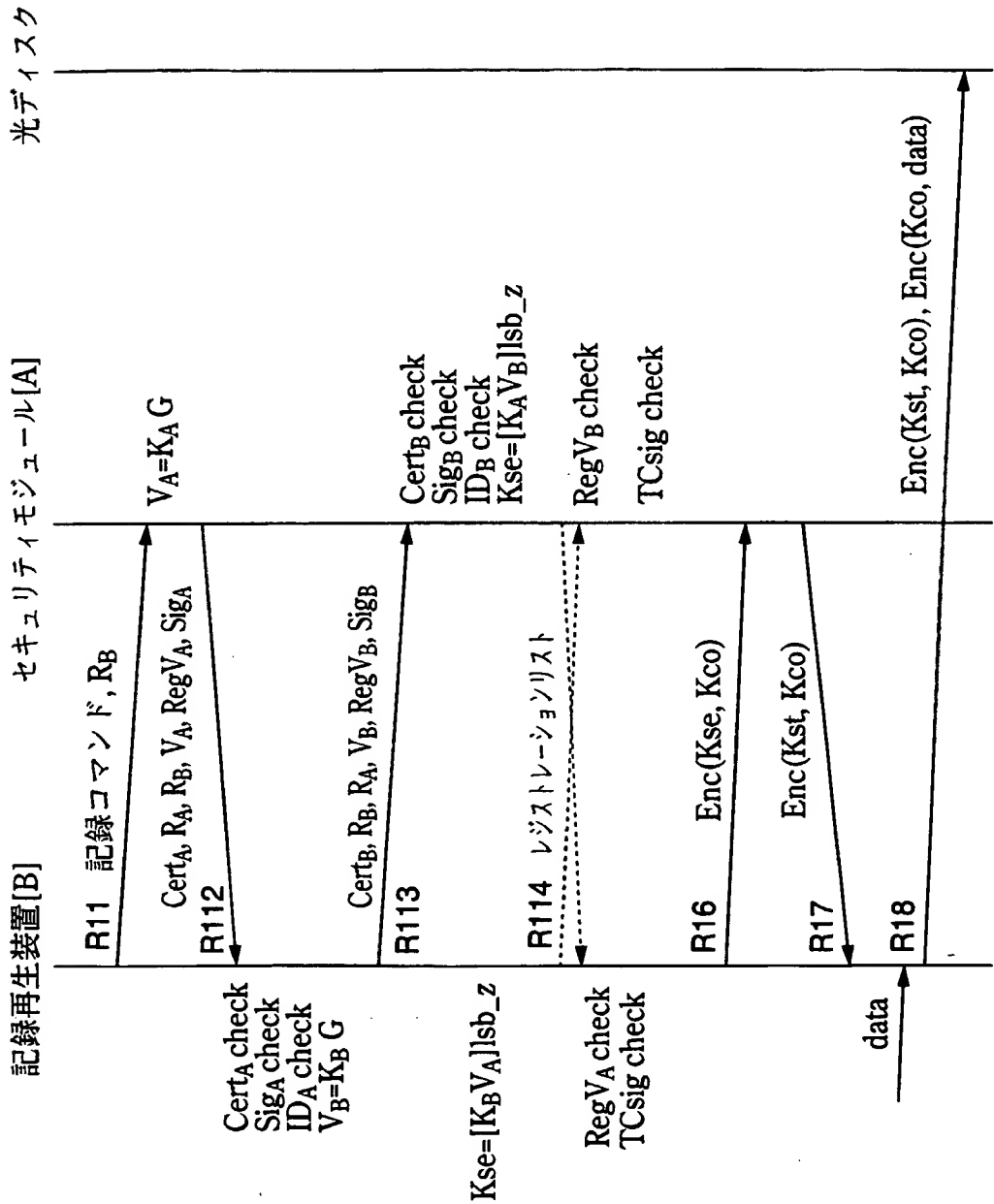


FIG.25

THIS PAGE BLANK (USE)

25/94

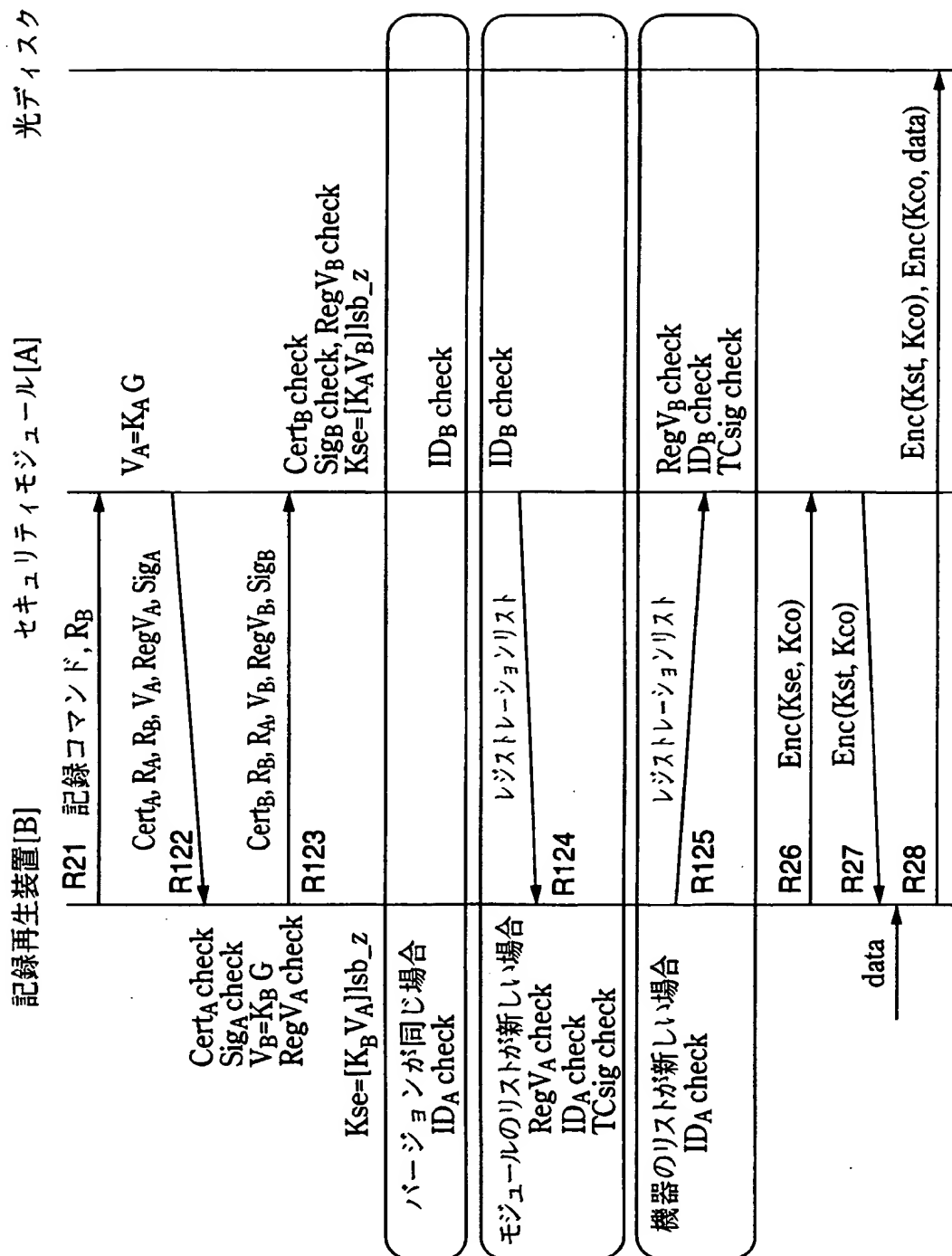


FIG.26

**THIS PAGE BLANK (USPTO)**

26/94

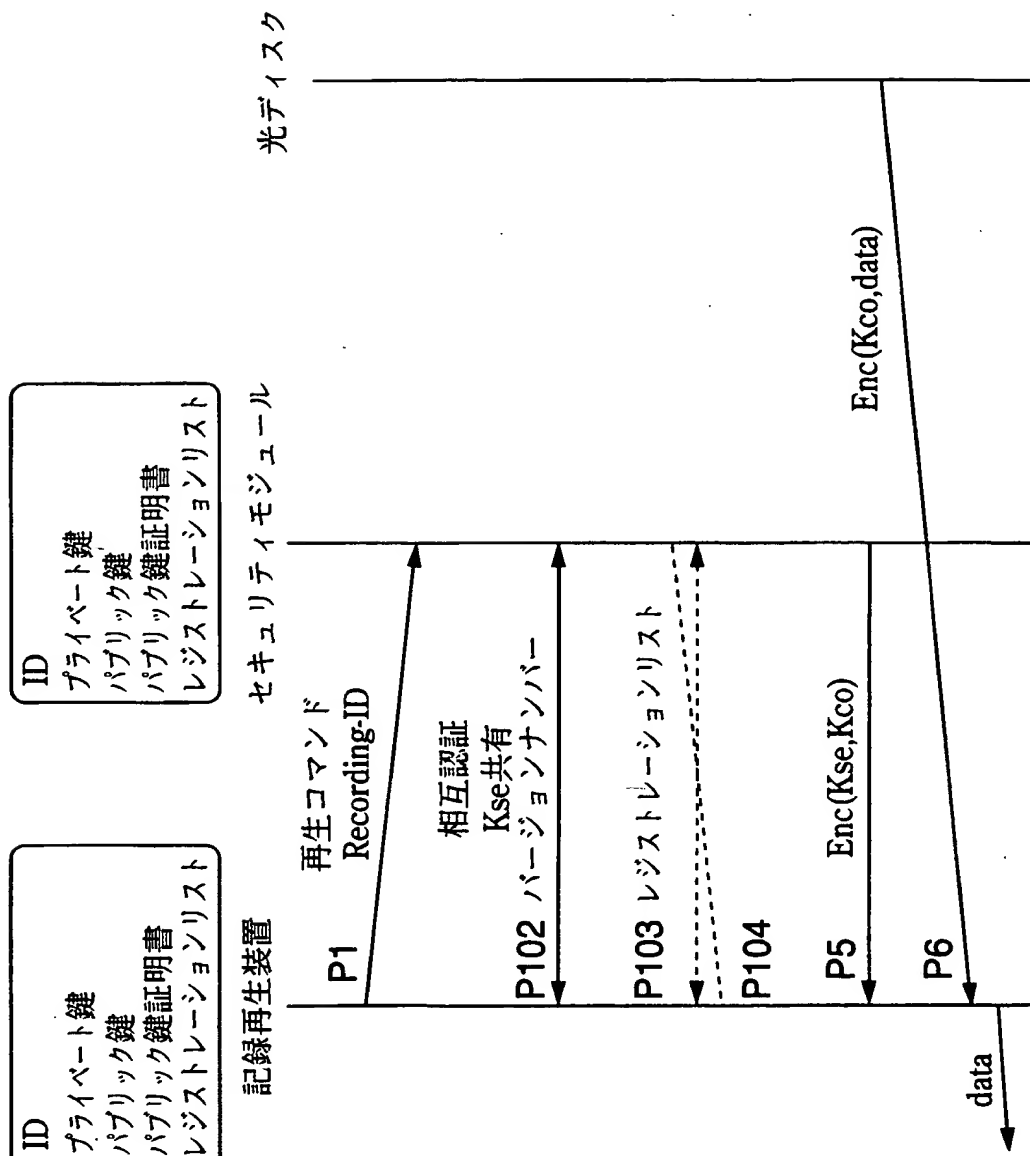


FIG.27

THIS PAGE BLANK (USPTO)

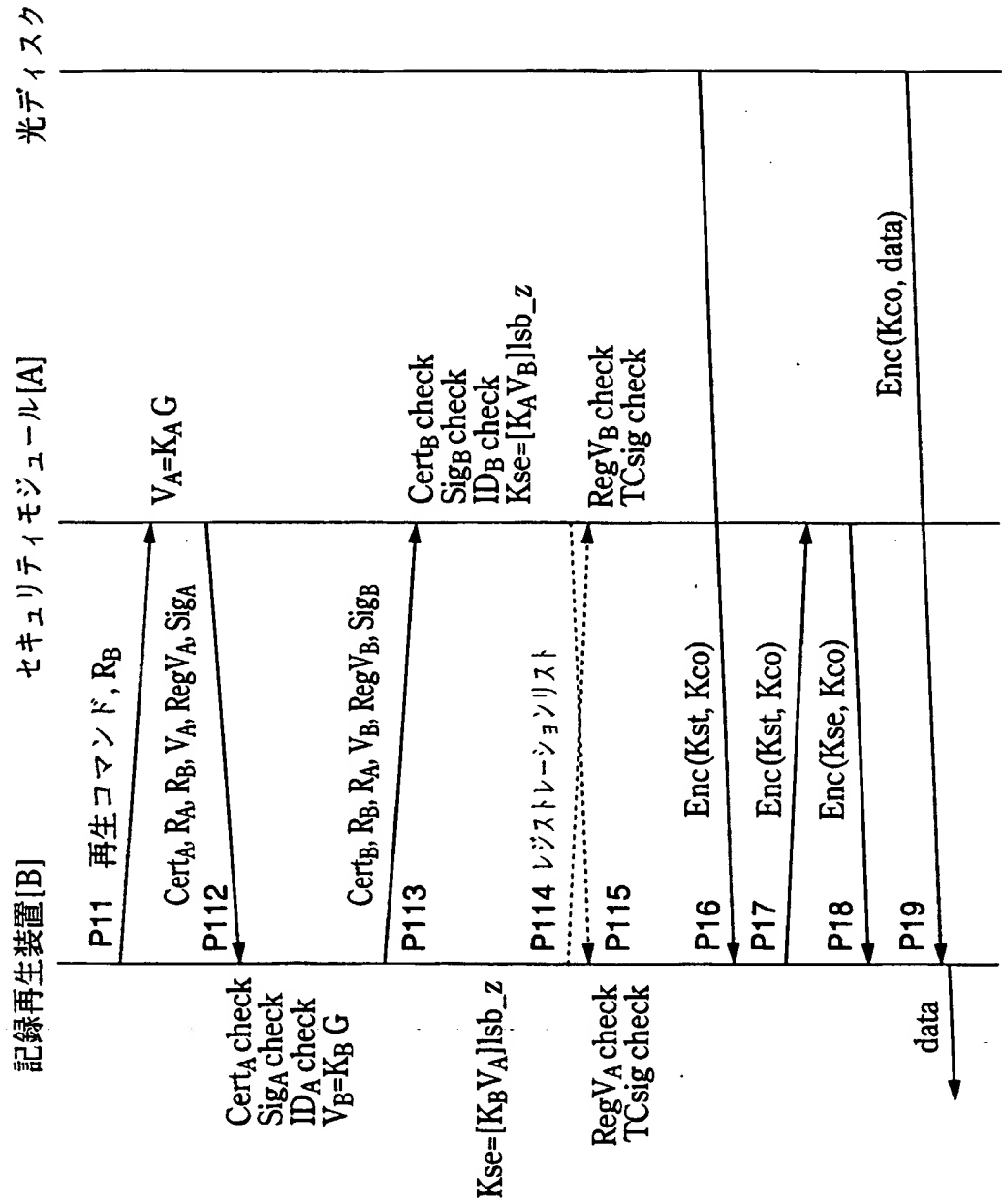


FIG.28

**THIS PAGE BLANK (USPTO)**



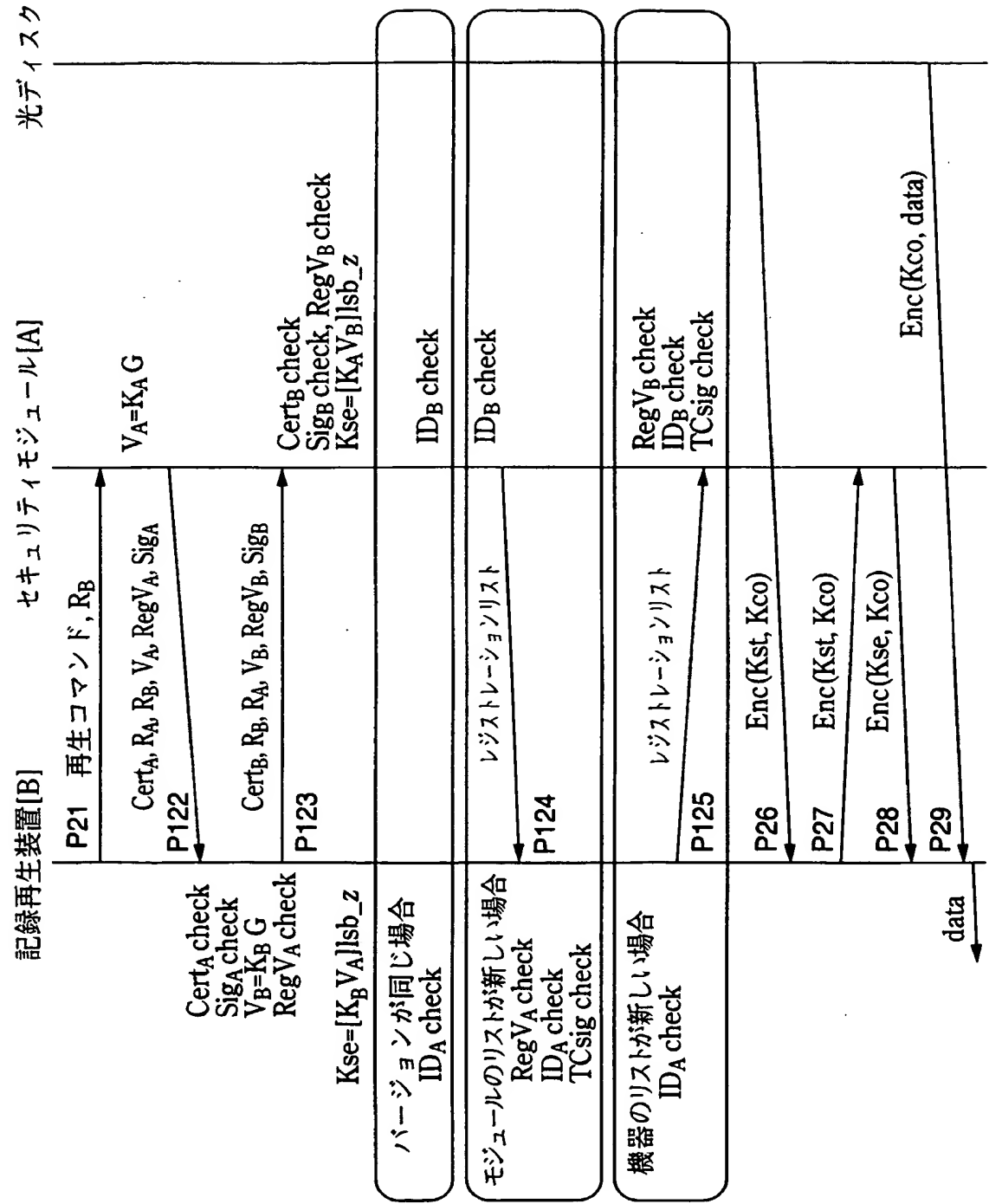


FIG.29

**THIS PAGE BLANK (USPTO)**

29/94

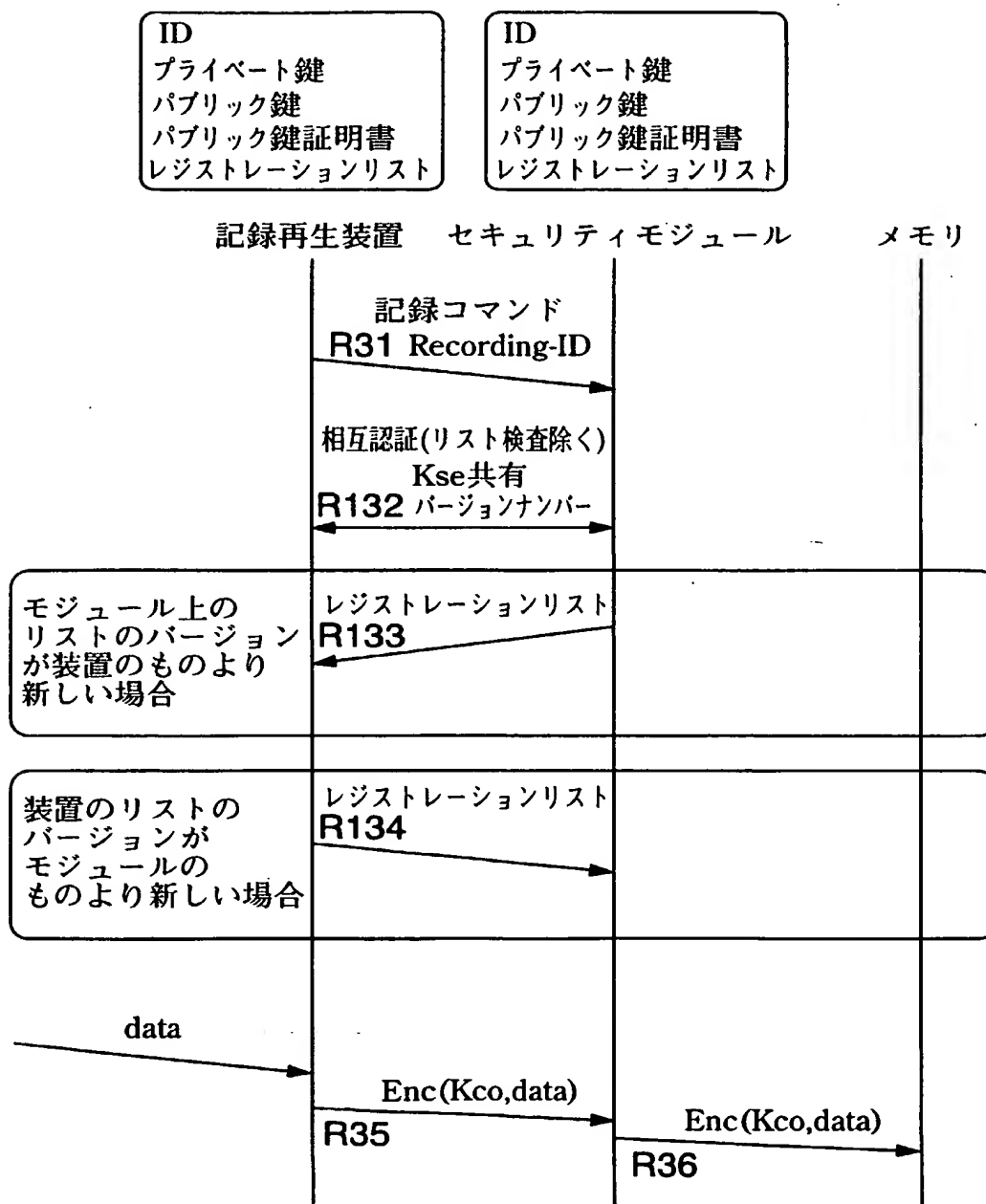


FIG.30

**THIS PAGE BLANK (USPTO)**

30/94

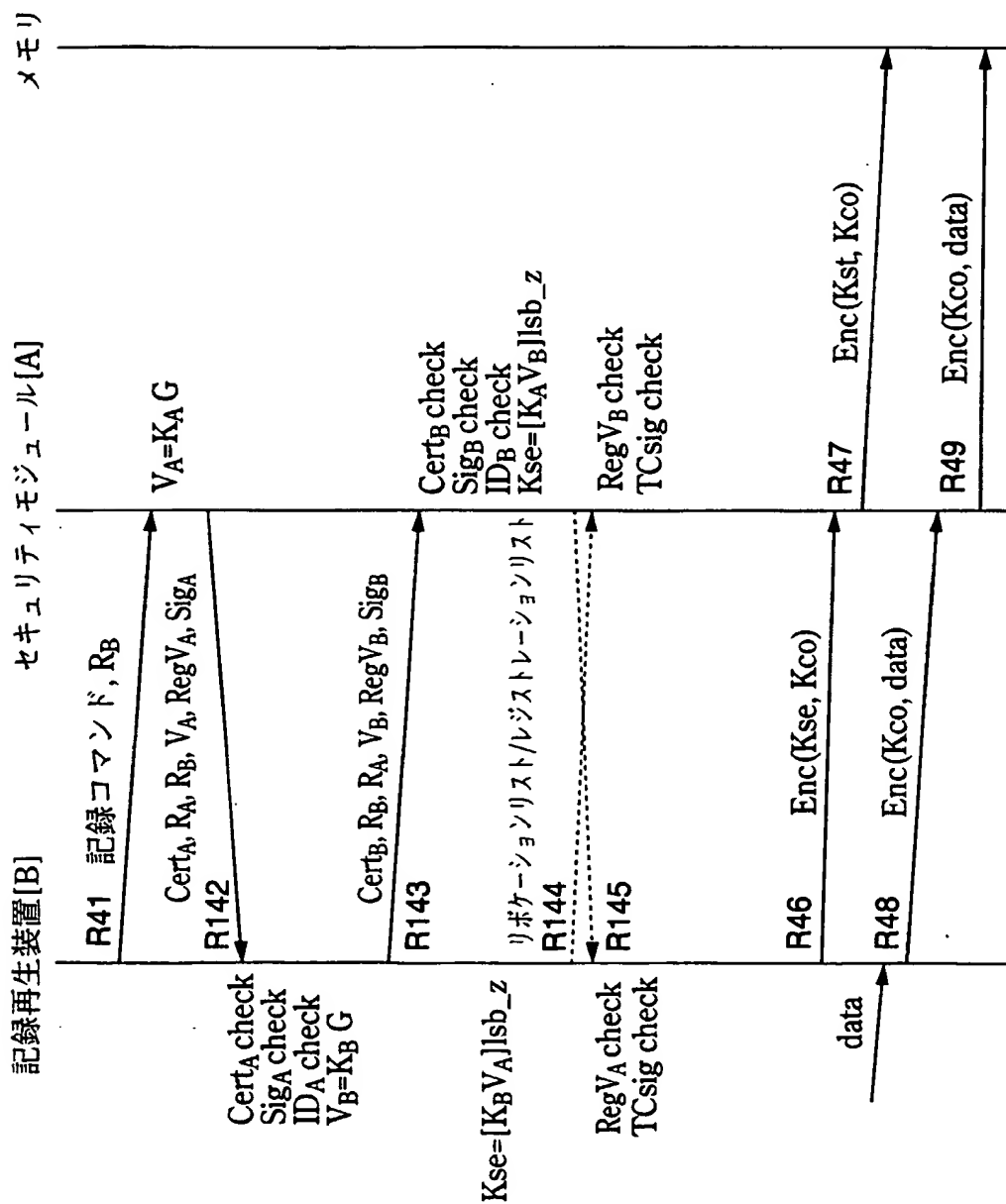


FIG.31

**THIS PAGE BLANK (USPTO)**

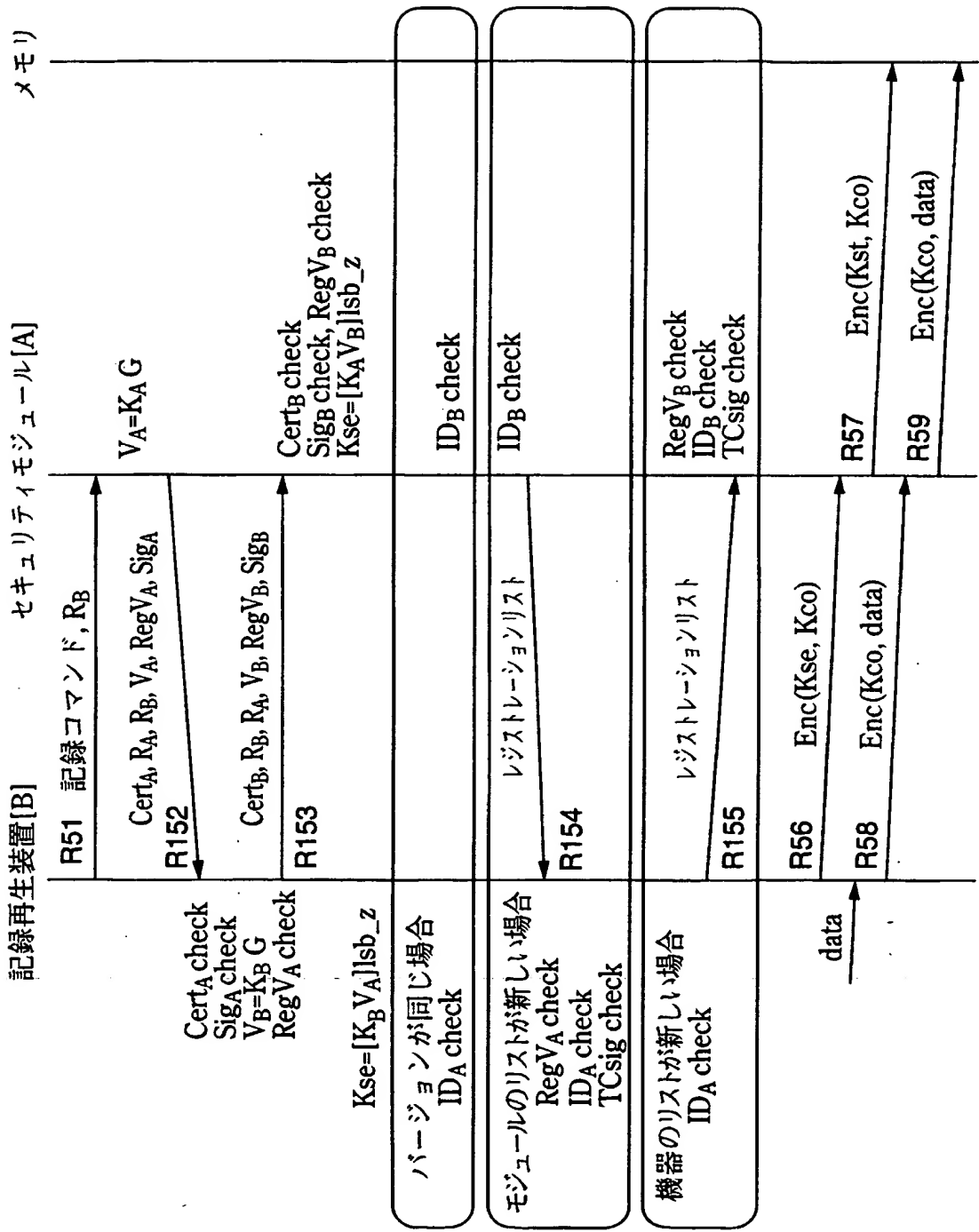


FIG.32

**THIS PAGE BLANK (USPTO)**



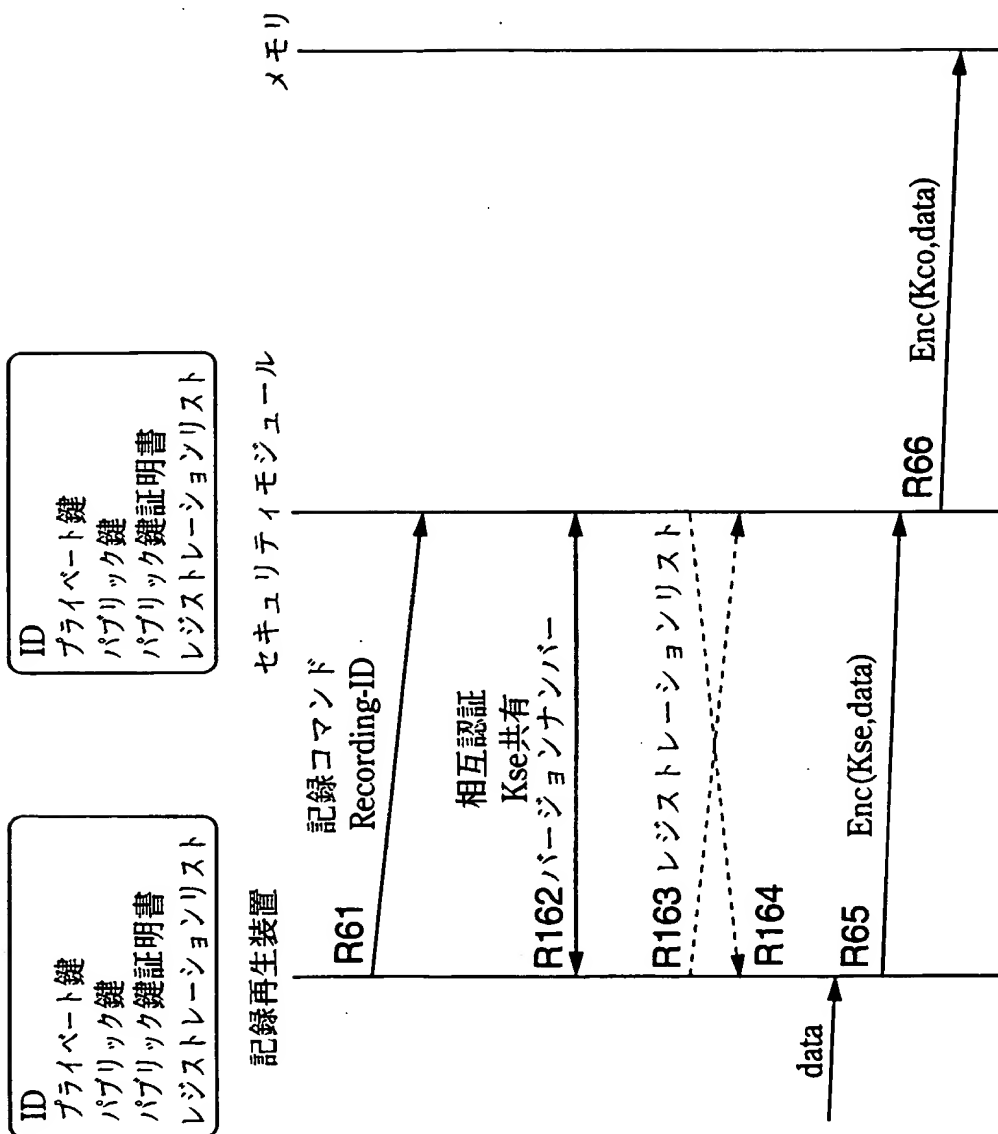


FIG.33

**THIS PAGE BLANK (USPTO)**

33/94

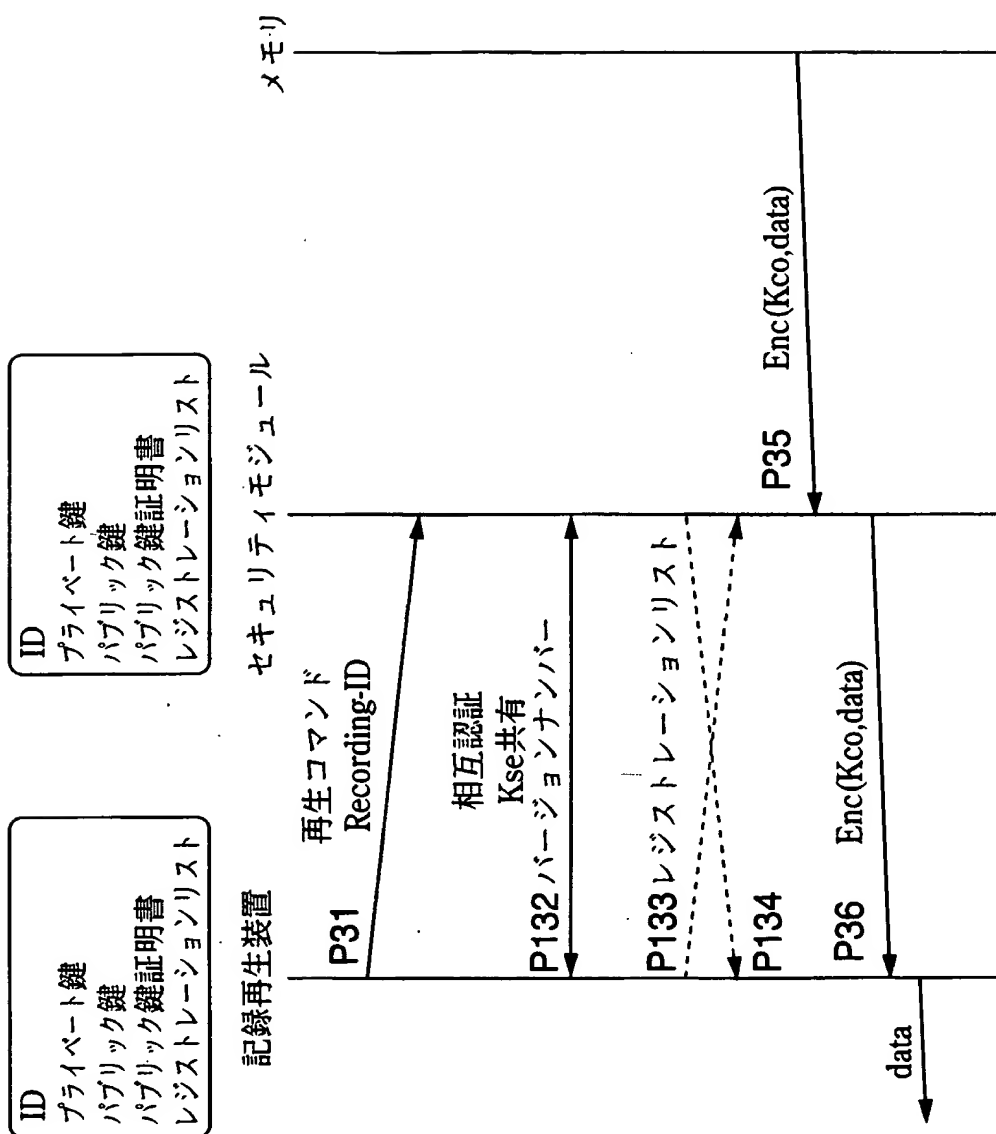


FIG.34

**THIS PAGE BLANK (USPTO)**

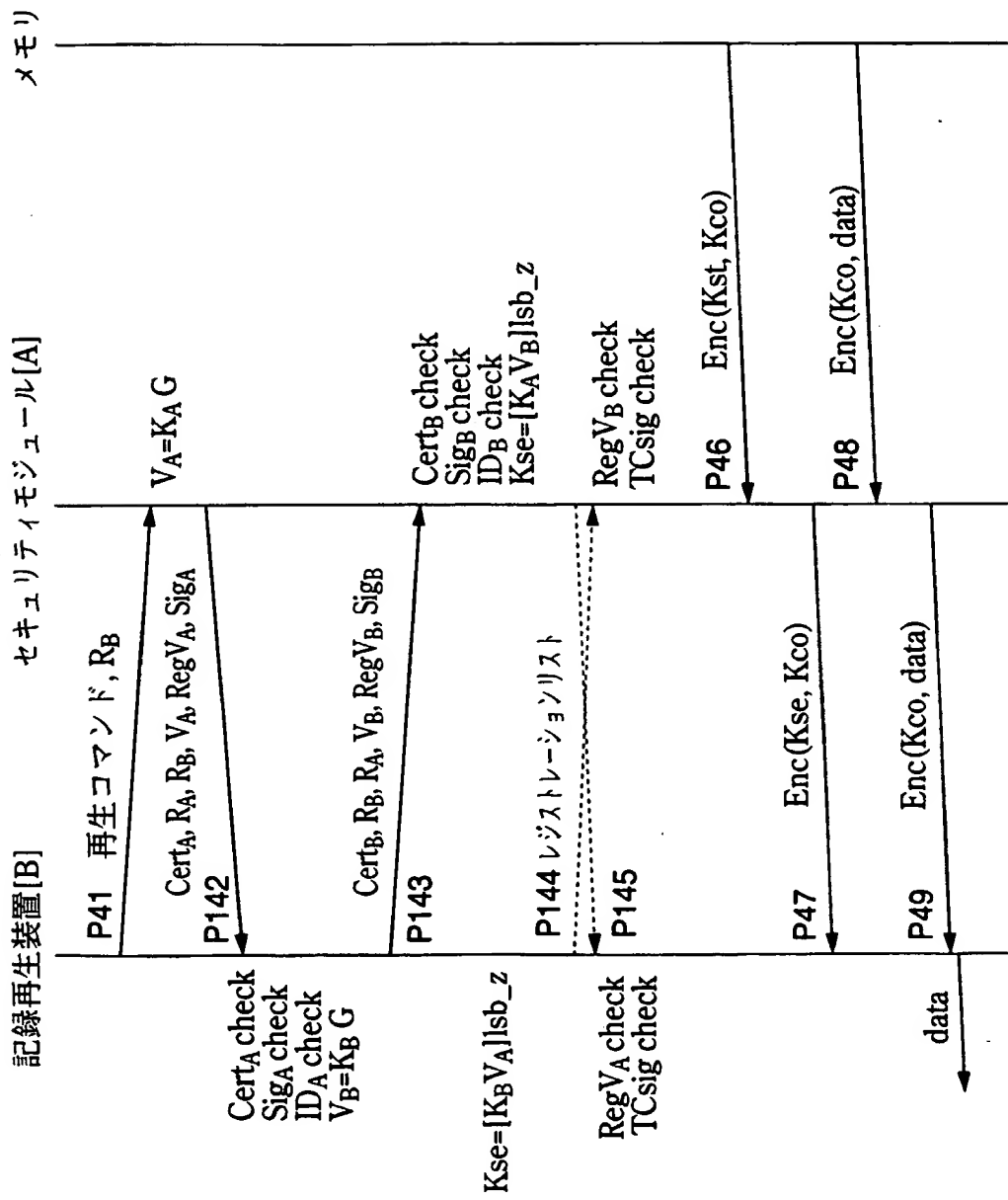


FIG.35

**THIS PAGE BLANK (USPTO)**

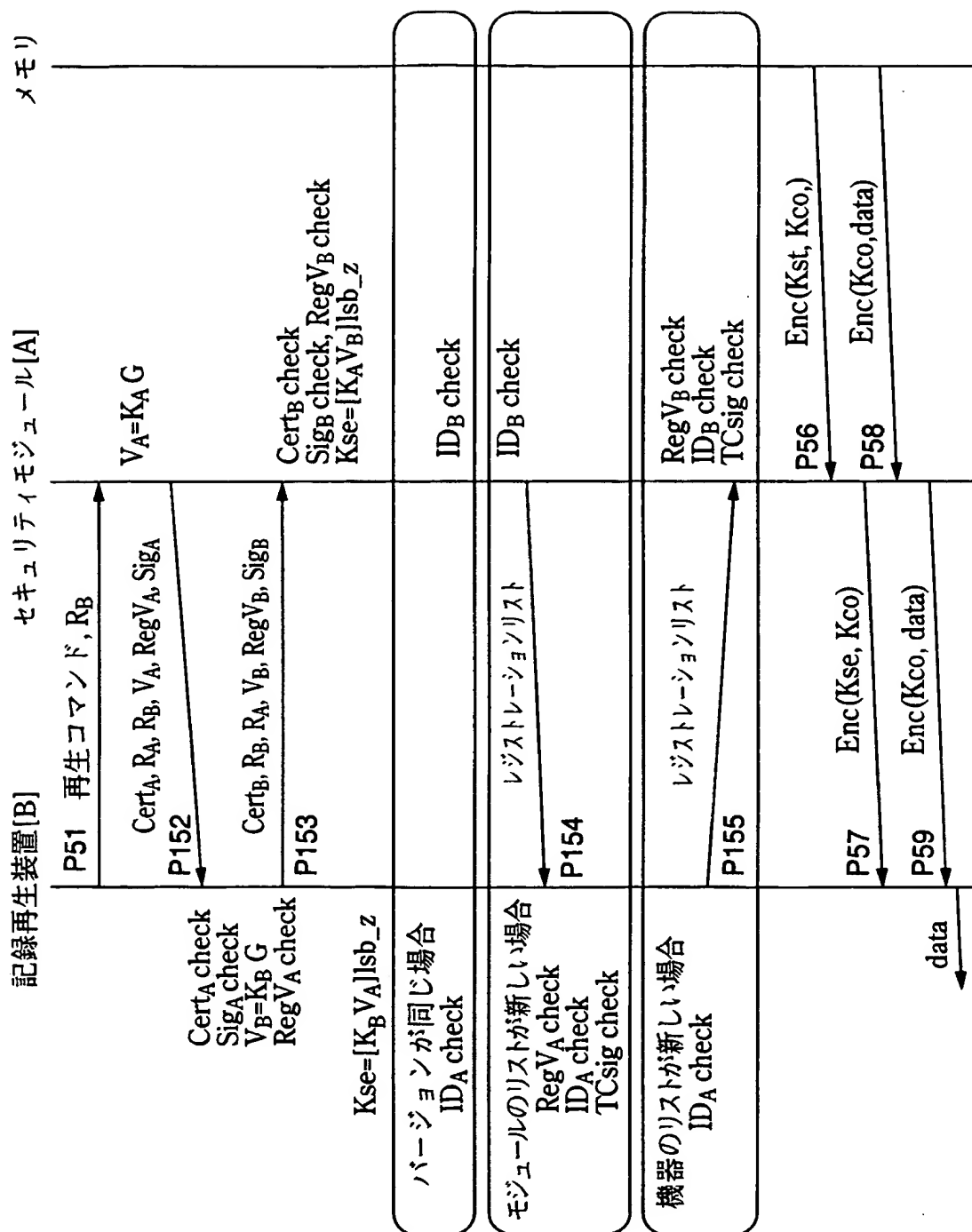


FIG.36

**THIS PAGE BLANK (USPTO)**



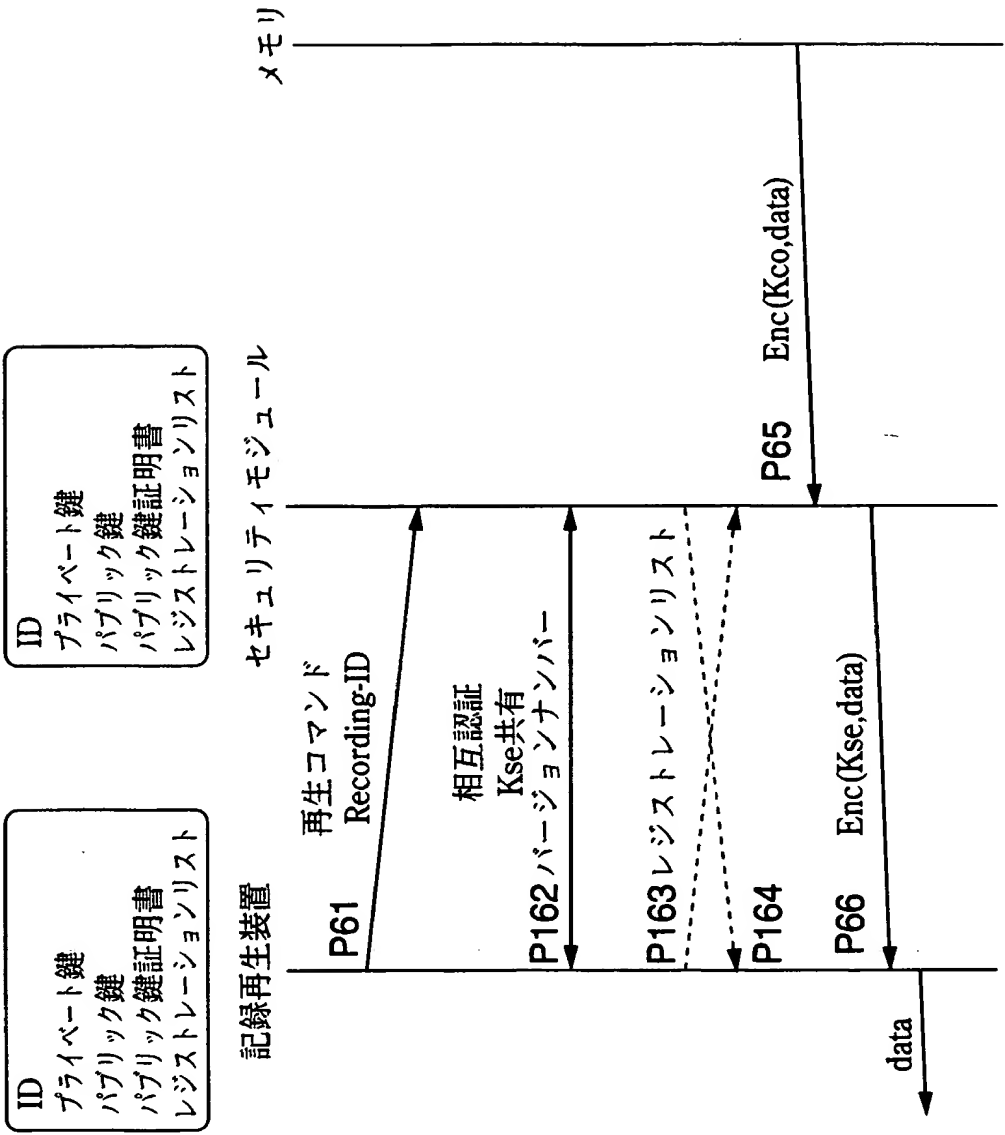


FIG.37

**THIS PAGE BLANK (USPTO)**

37/94

リボケーションリスト／レジストレーションリスト区別
バージョンナンバー
リボークされる機器または媒体のID（リボケーションリスト）， 登録される機器または媒体のID（レジストレーションリスト）
．．．．．
TCのデジタル署名

FIG.38

**THIS PAGE BLANK (USPTO)**

38/94

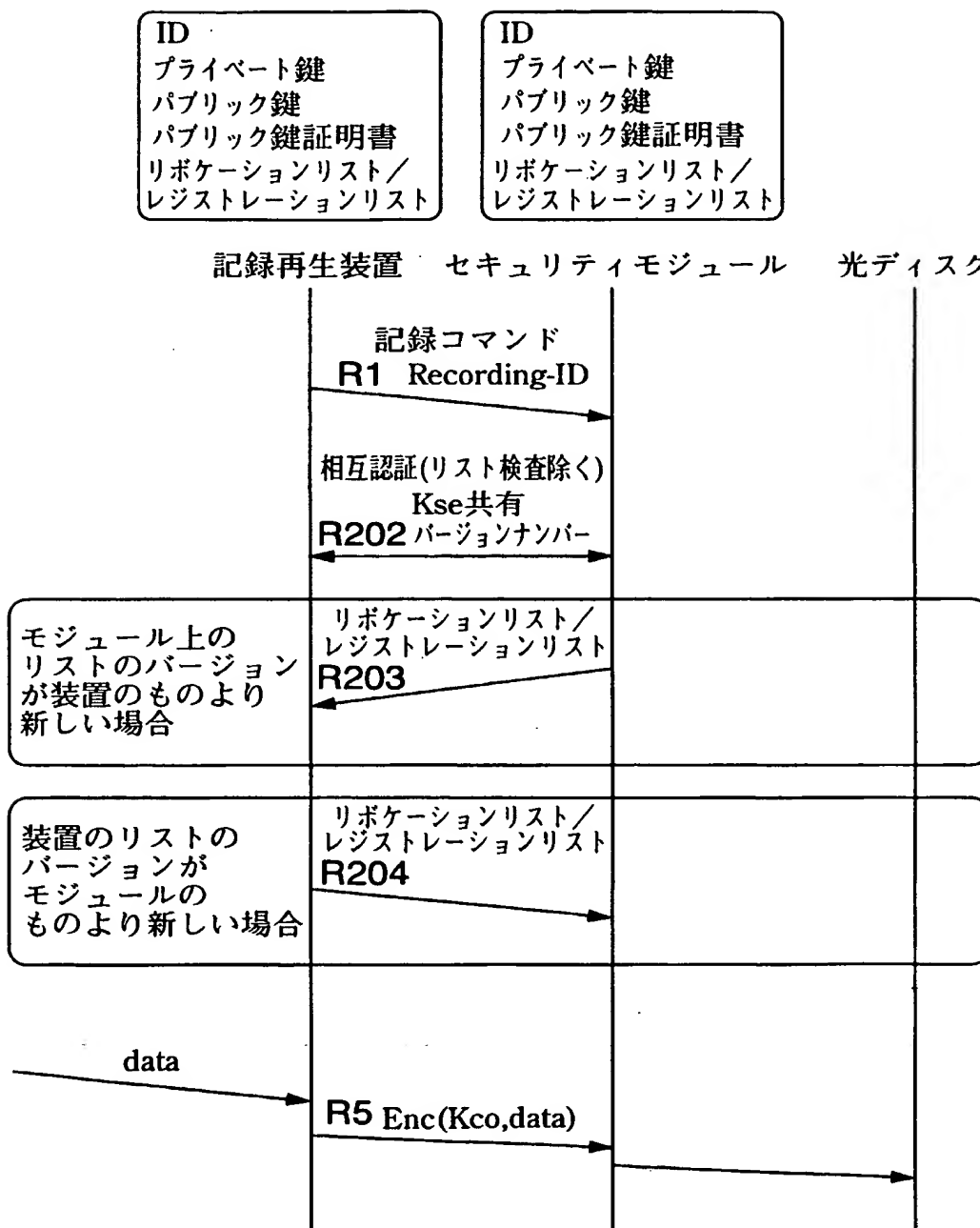


FIG.39

**THIS PAGE BLANK (USP)**

39/94

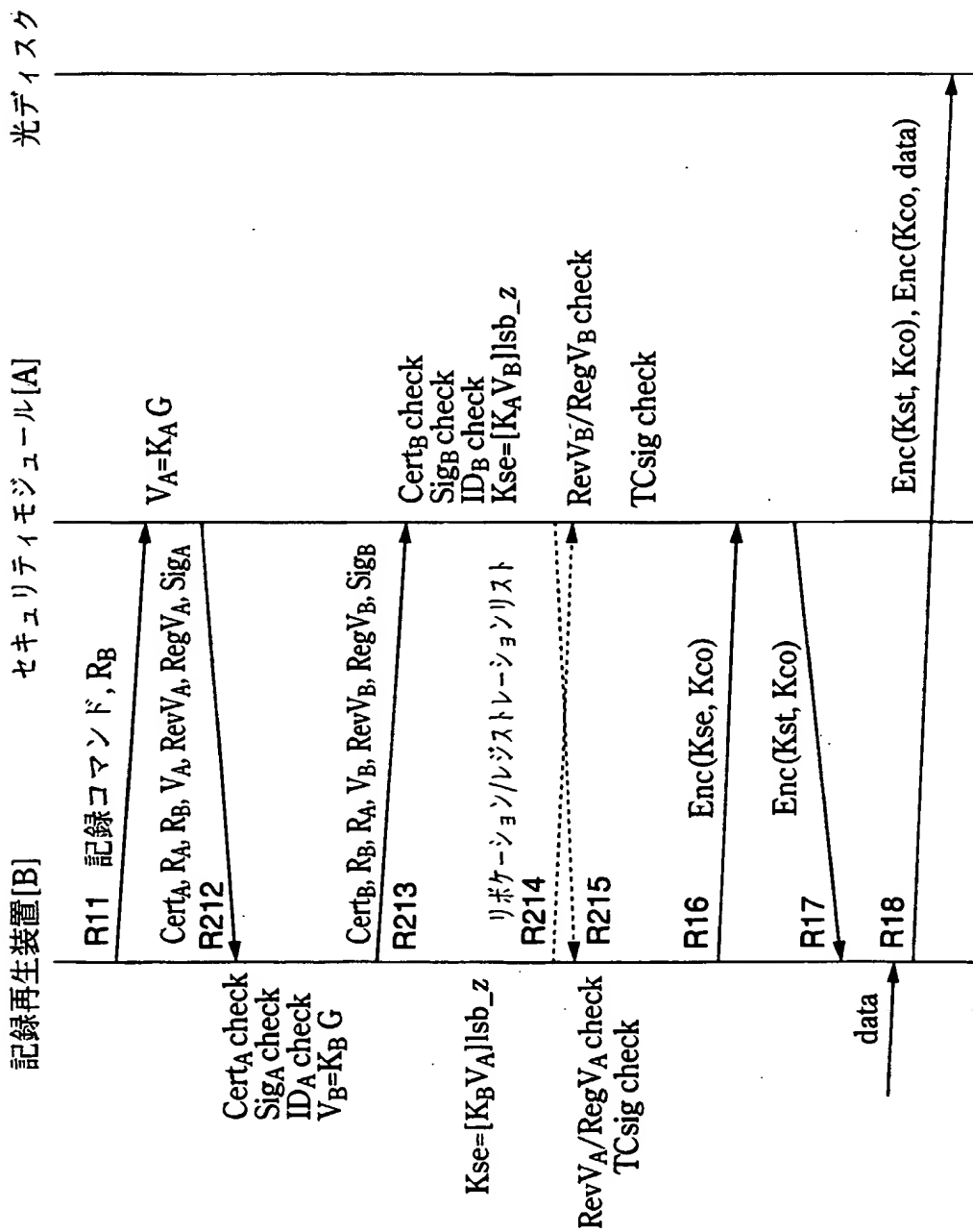


FIG.40

**HIS PAGE BLANK (USPTO)**



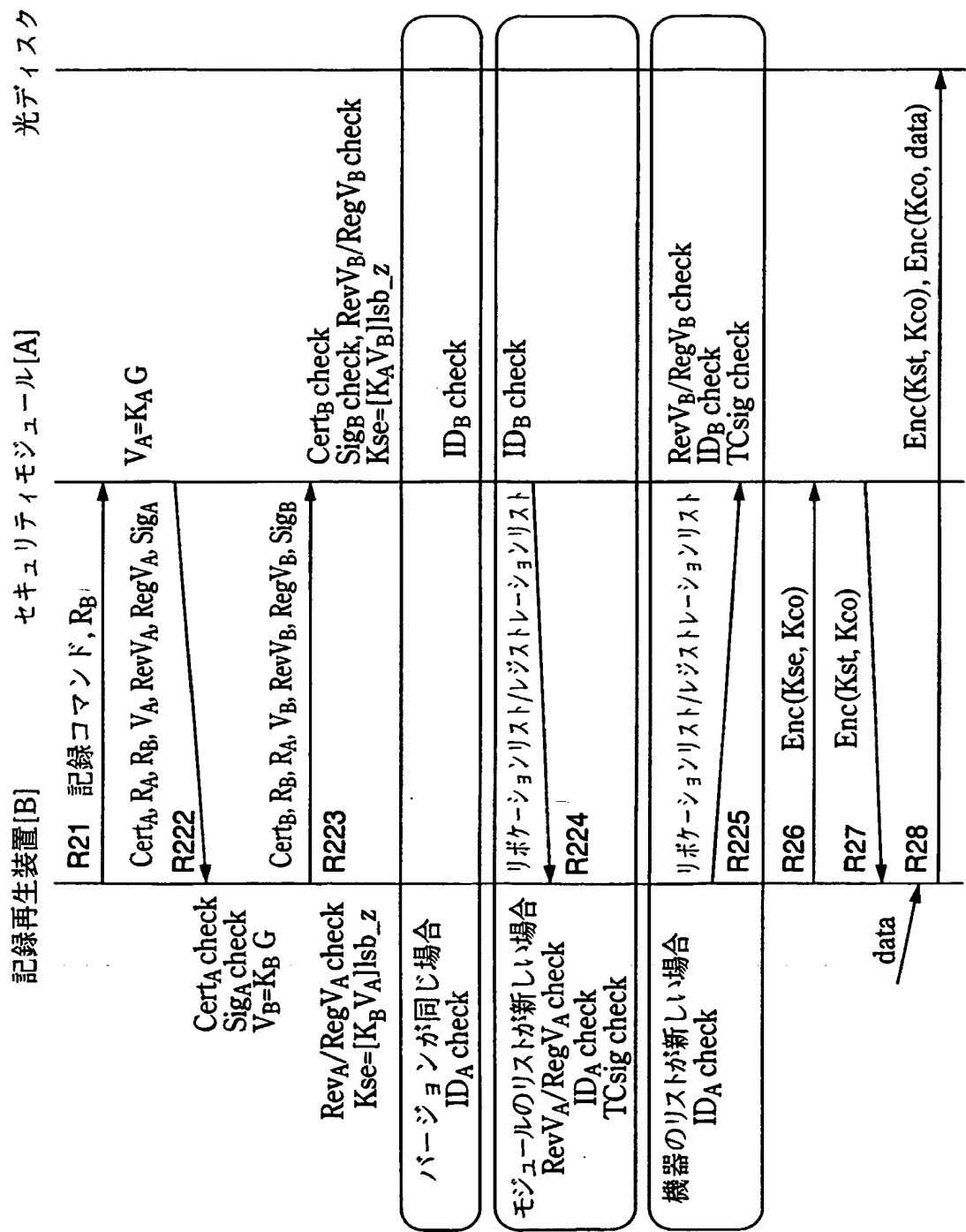


FIG.41

**THIS PAGE BLANK (USPTO)**

**THIS PAGE BLANK (USPTO)**

41/94

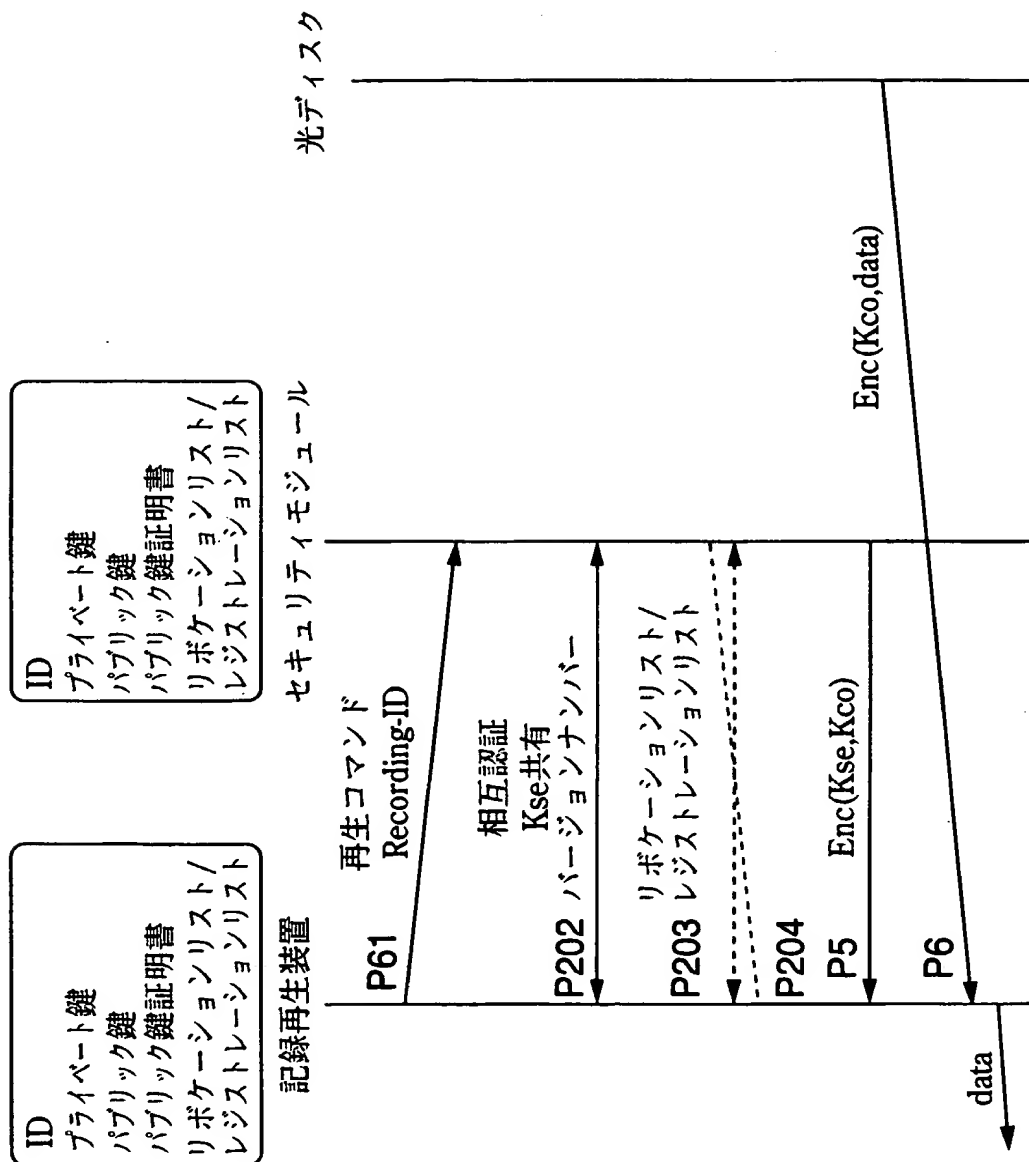


FIG.42

**THIS PAGE BLANK (USPTO)**

42/94

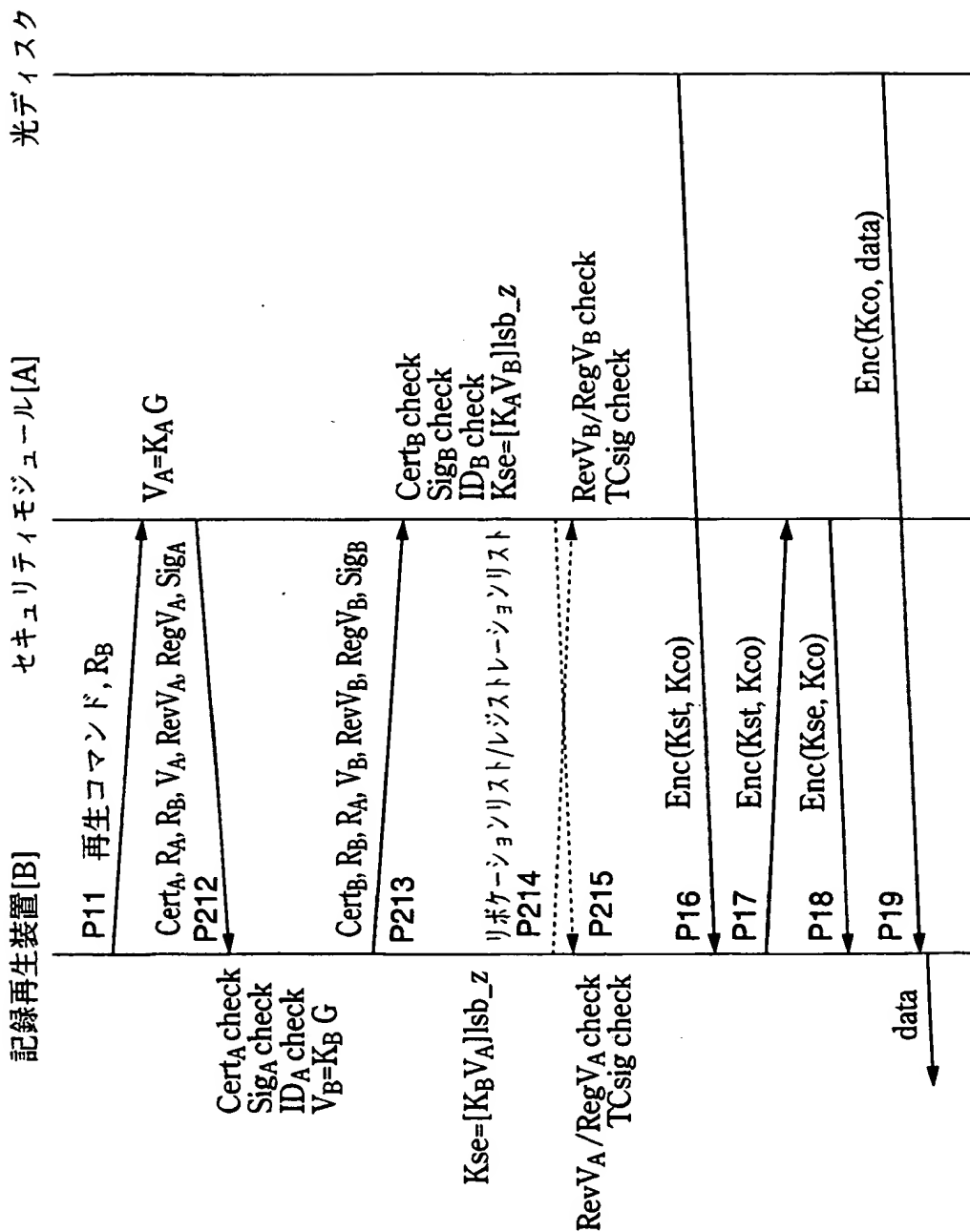


FIG.43

**THIS PAGE BLANK (USPTO)**

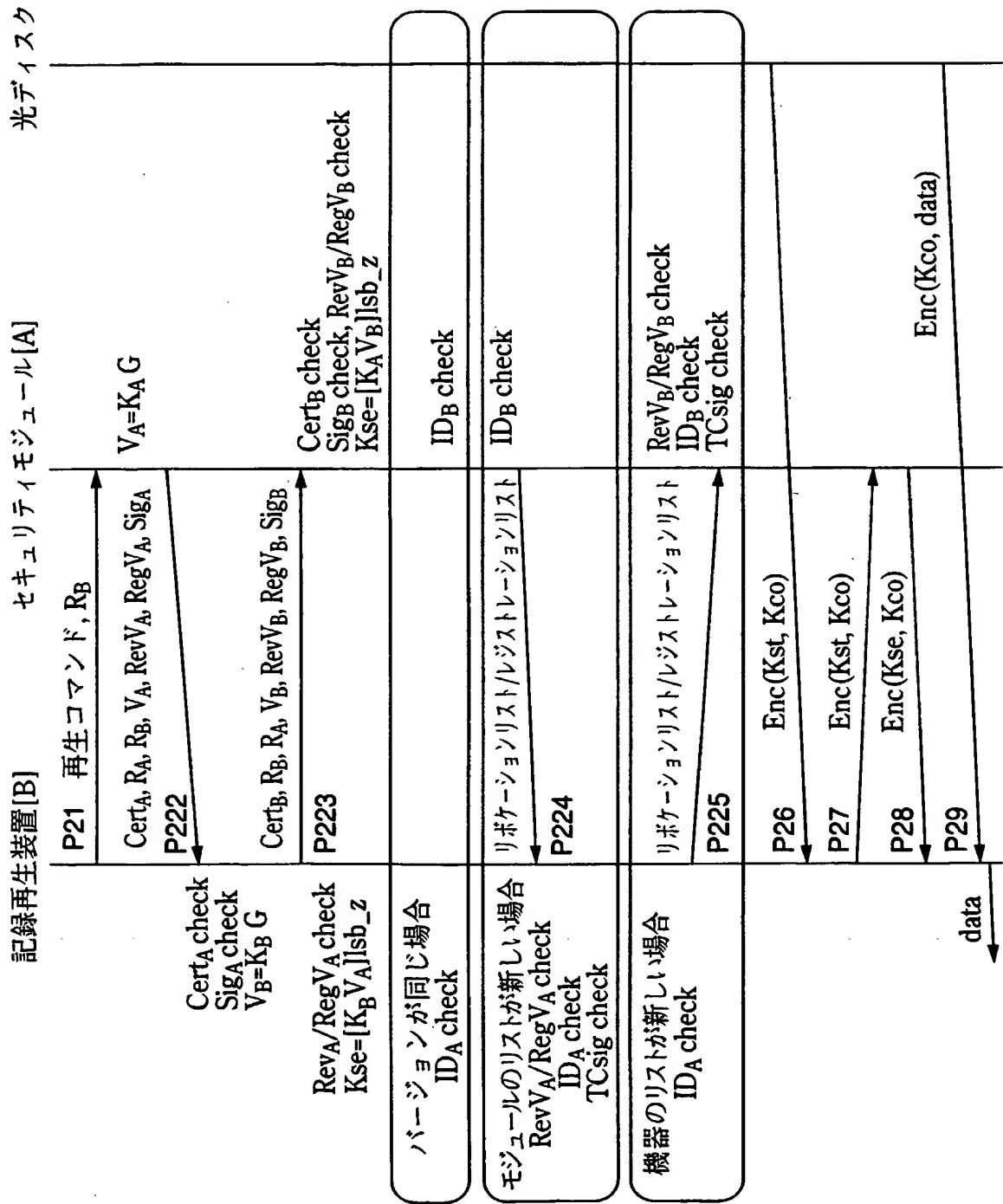


FIG.44

**THIS PAGE BLANK (USPTO)**



44/94

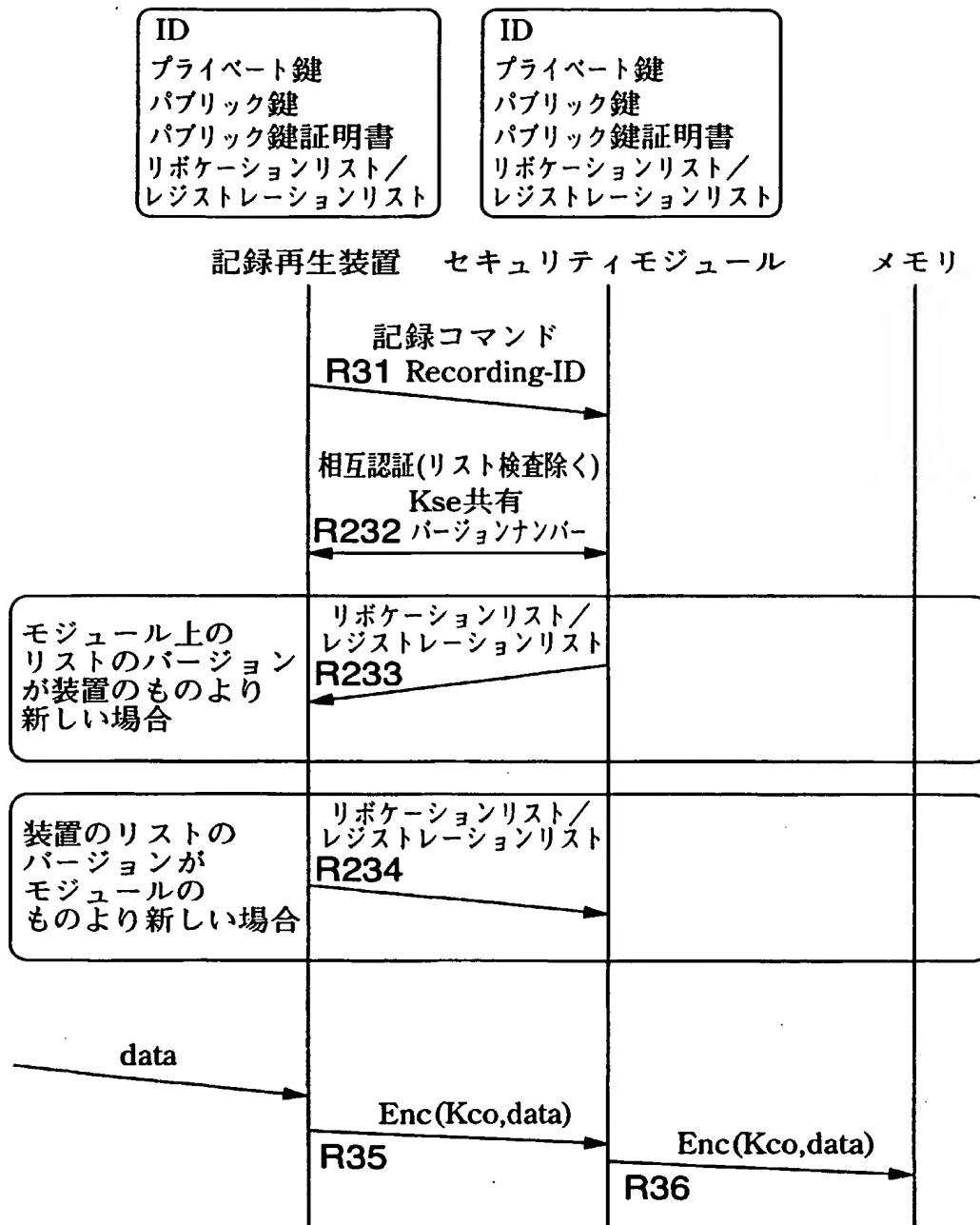


FIG.45

**THIS PAGE BLANK (USPTO)**

45/94

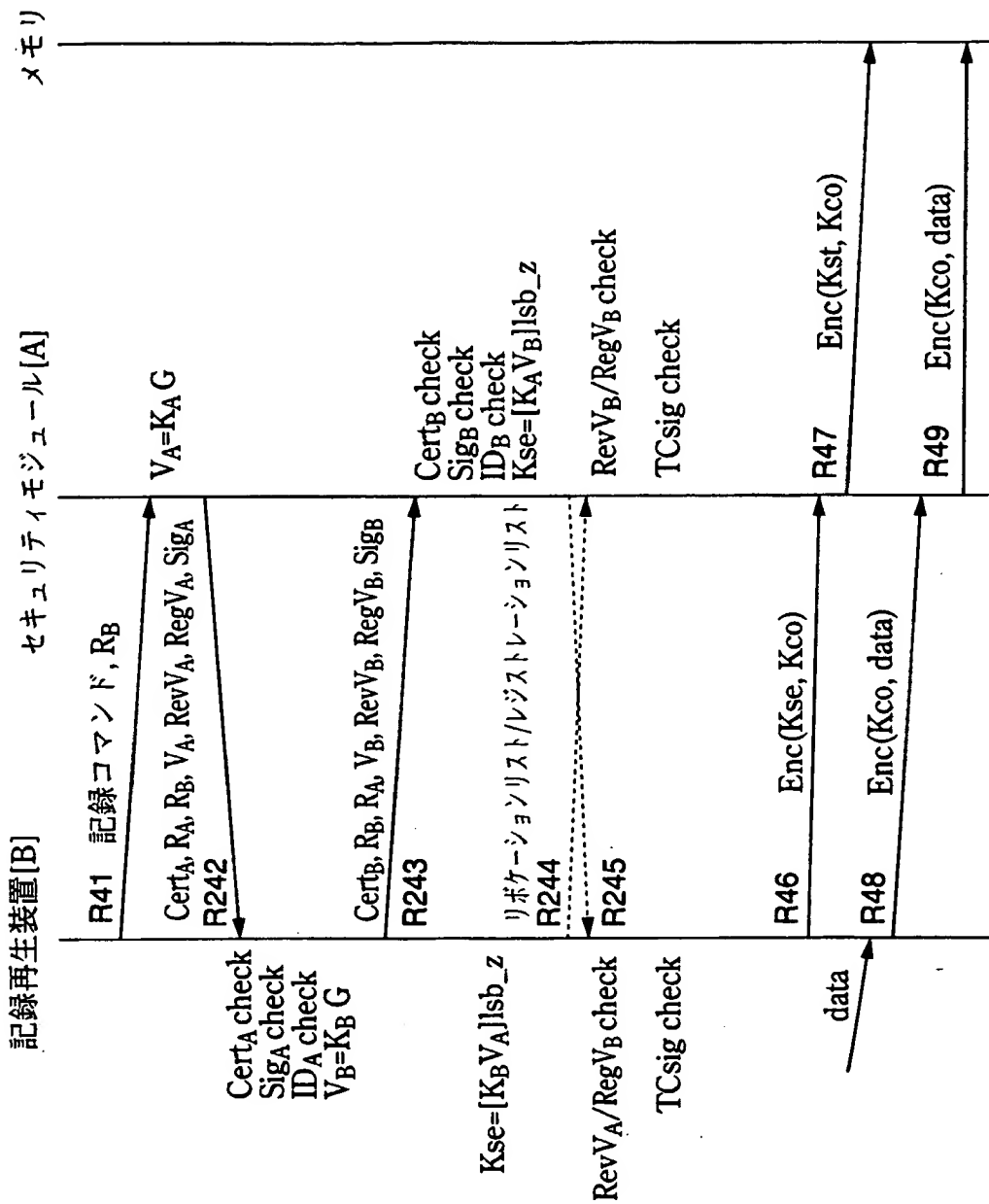


FIG.46

**THIS PAGE BLANK (USPTO)**

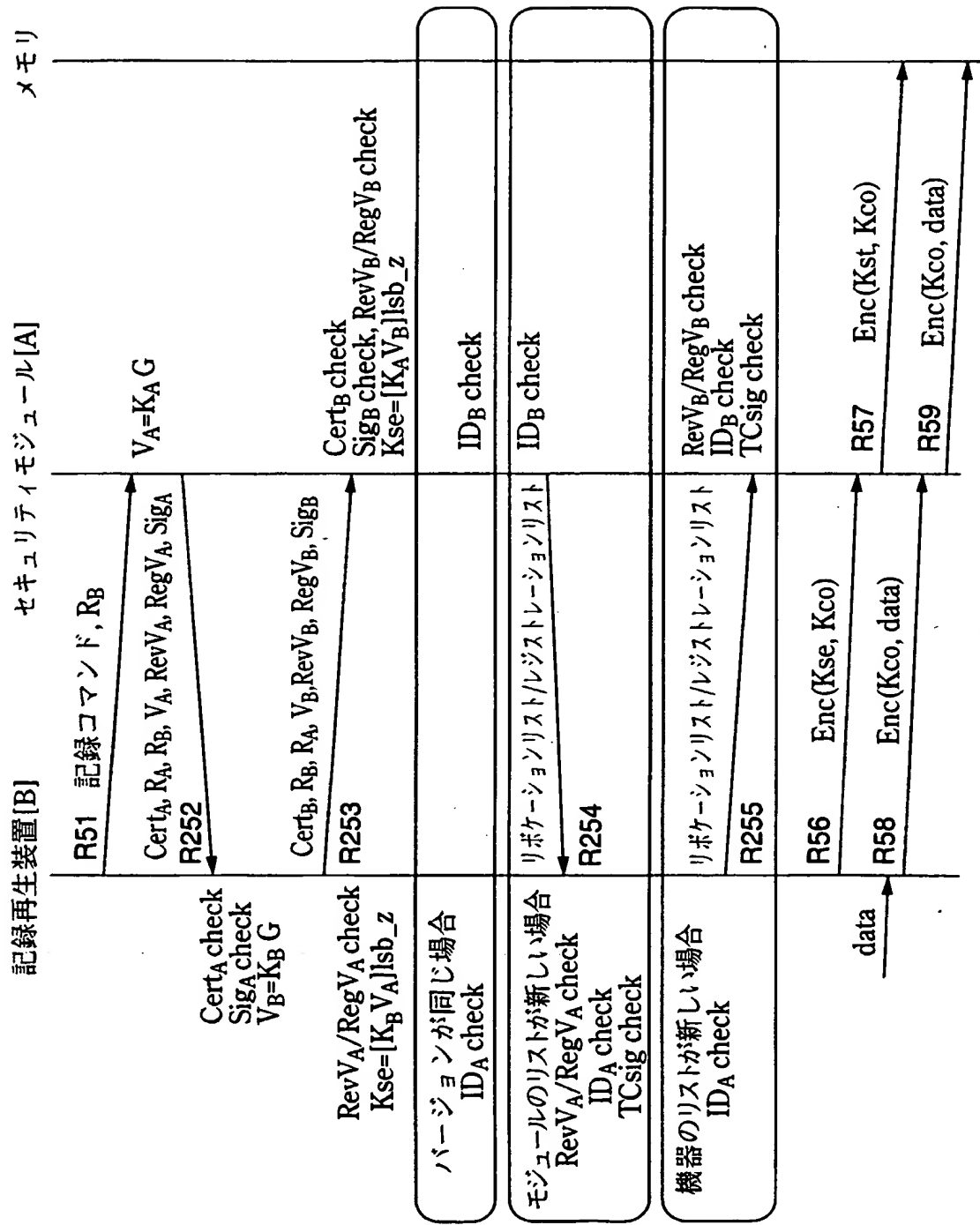


FIG.47

**THIS PAGE BLANK (USPTO)**

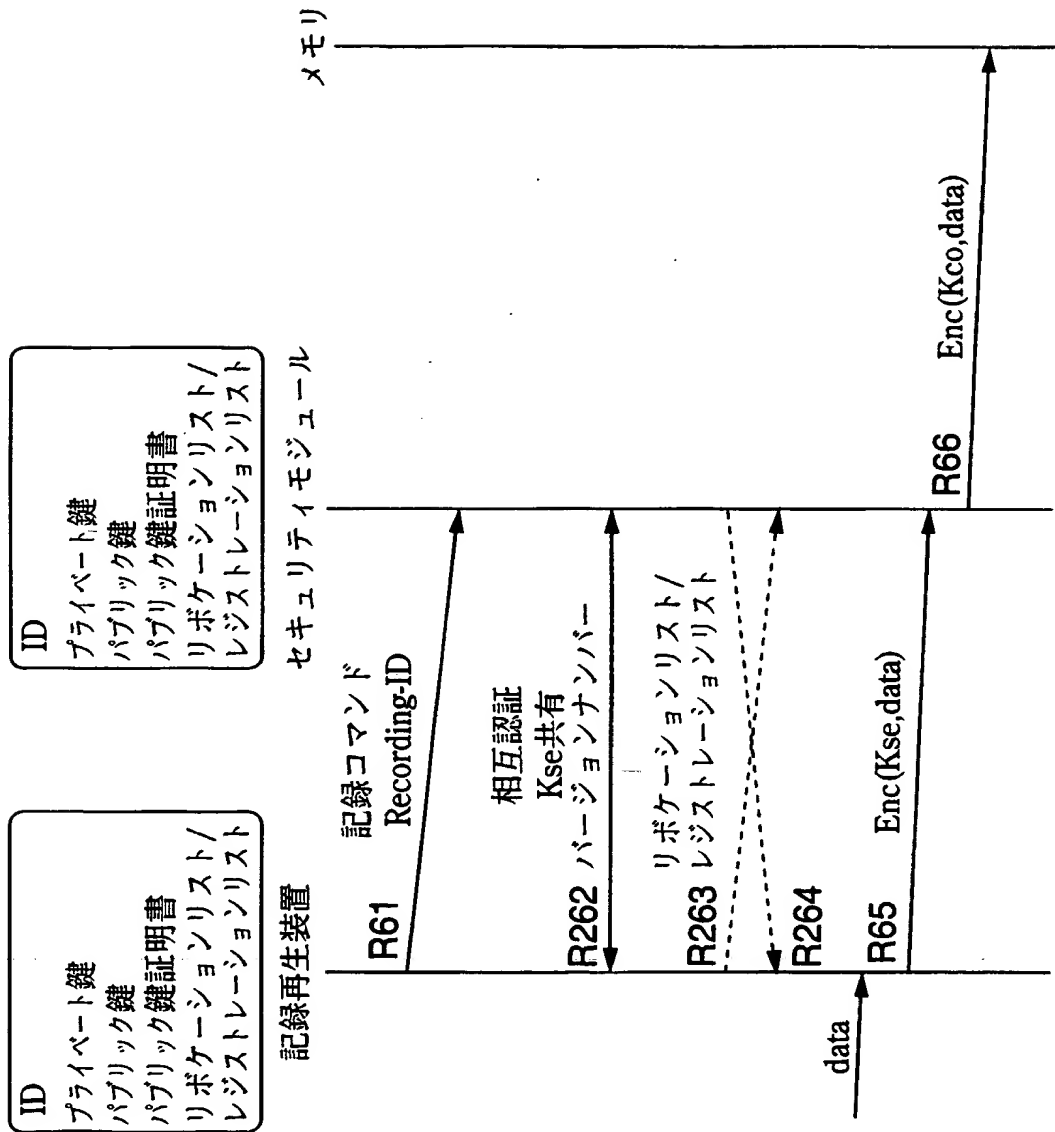


FIG.48

**THIS PAGE BLANK (USPTO)**



48/94

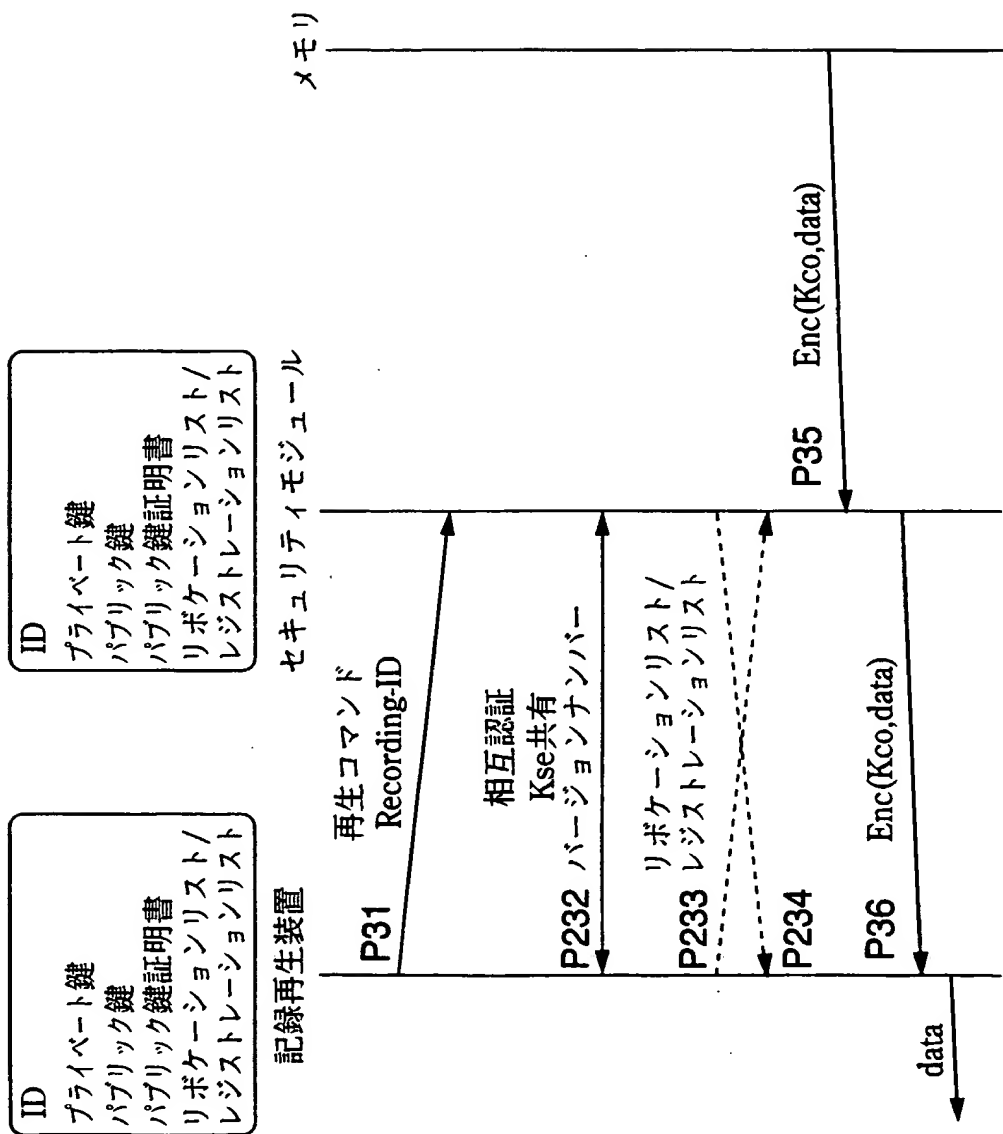


FIG.49

**THIS PAGE BLANK (USPTO)**

49/94

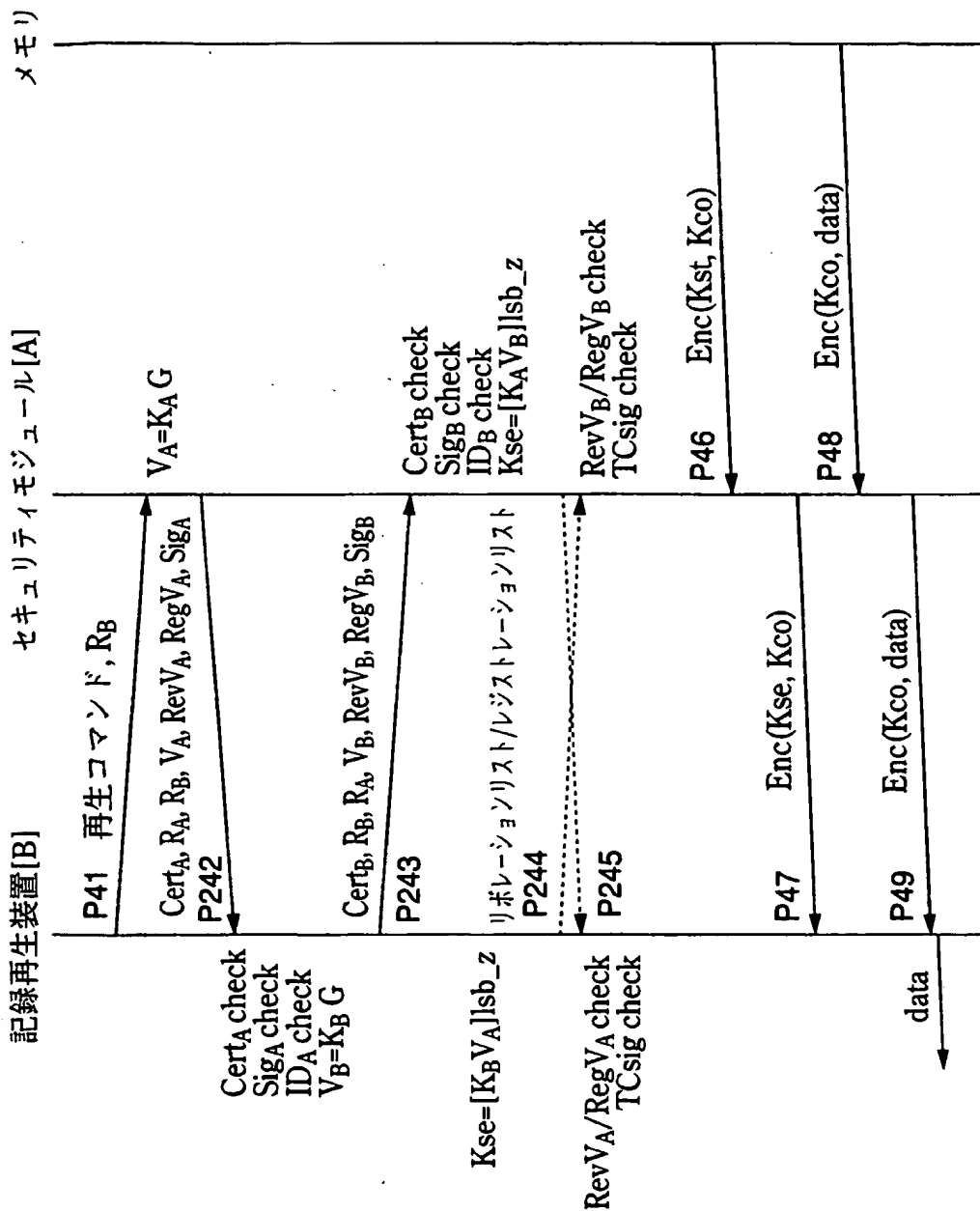


FIG.50

**THIS PAGE BLANK (USPTO)**

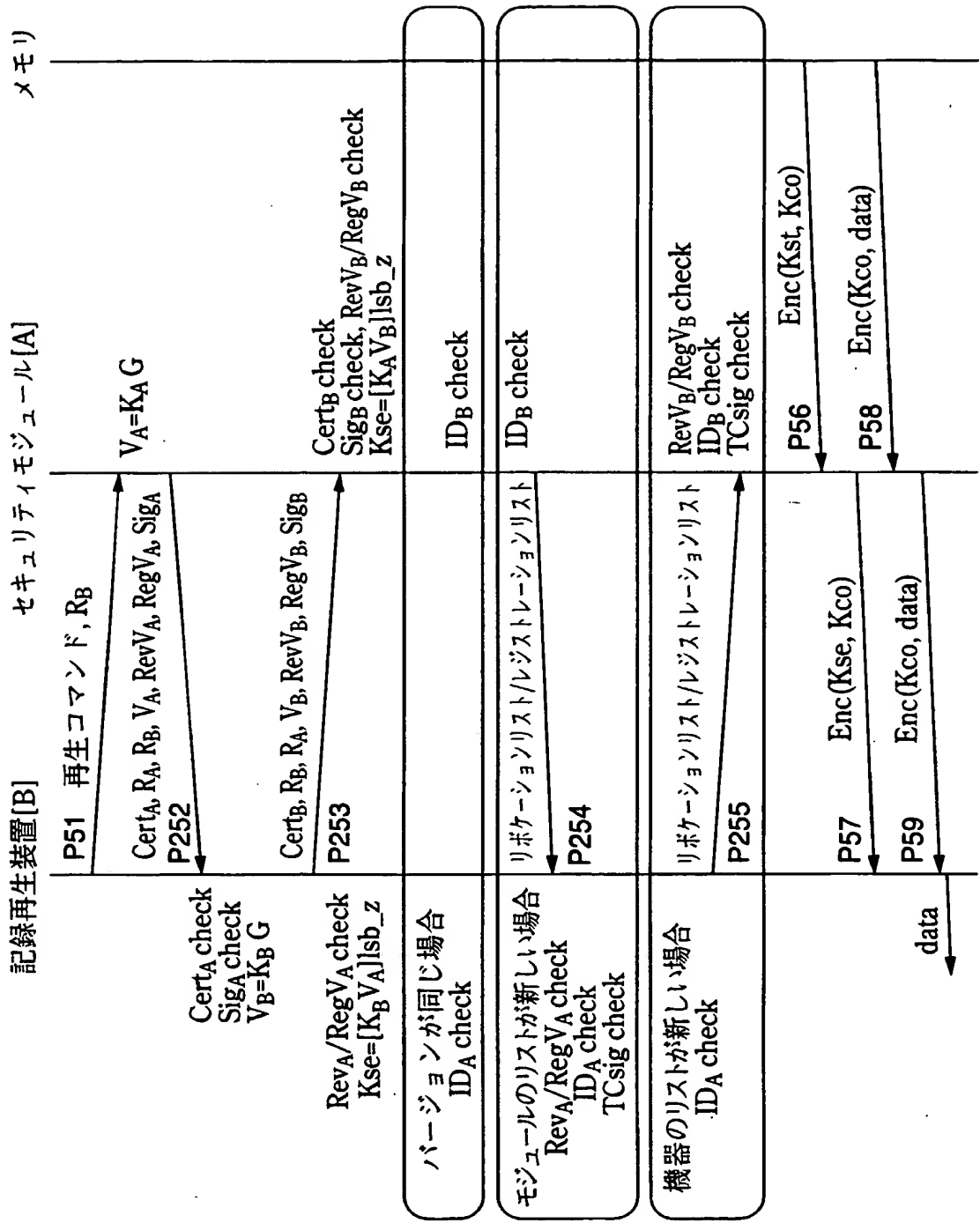


FIG.51

**THIS PAGE BLANK (USPTO)**

51/94

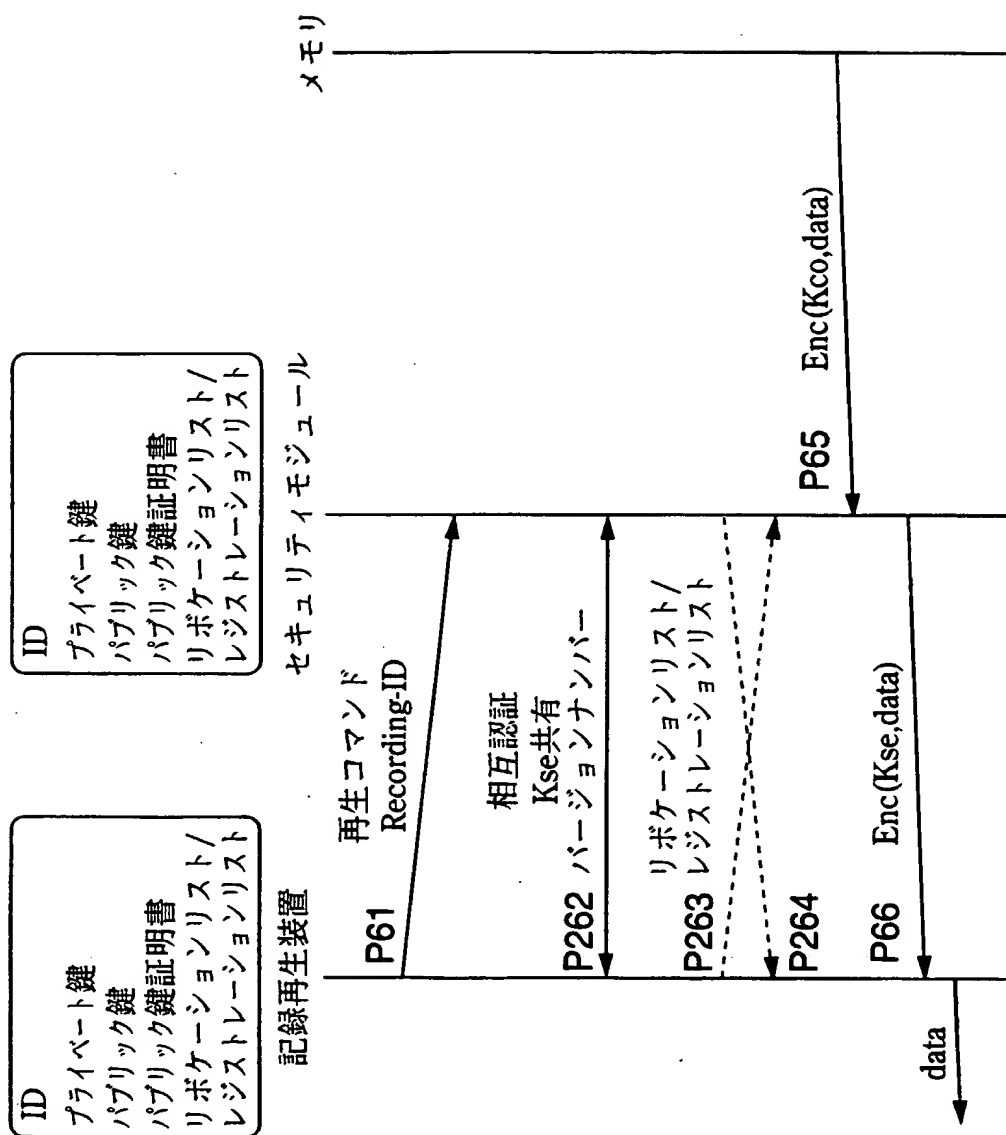
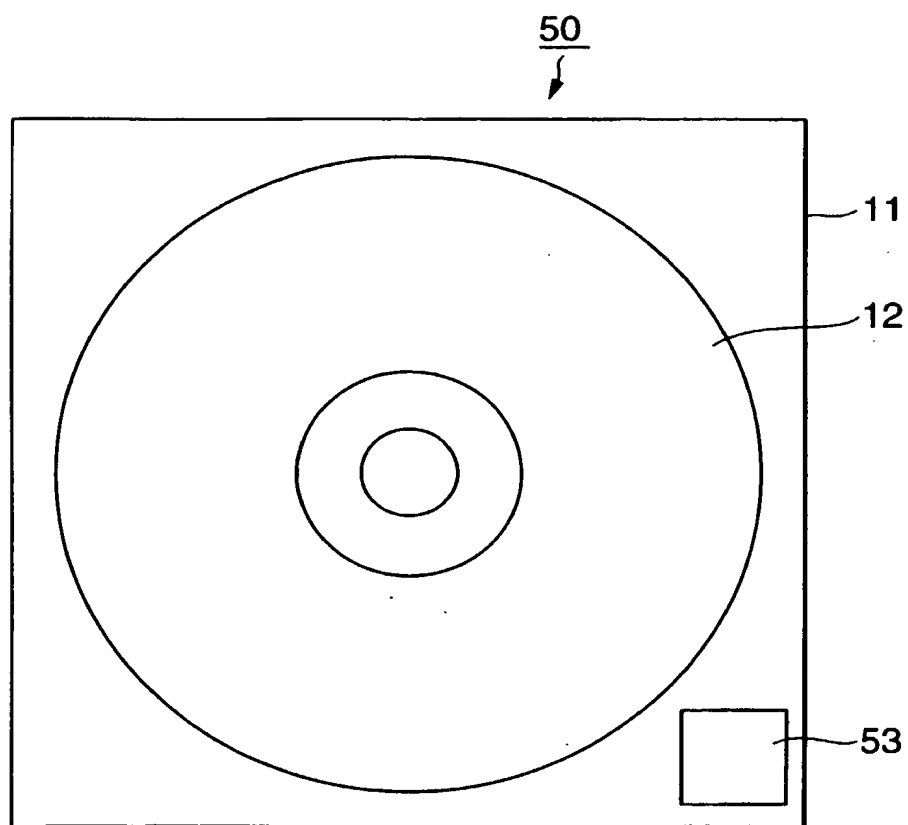


FIG.52

**THIS PAGE BLANK (USPTO)**



52/94



**FIG.53**

**THIS PAGE BLANK (USPTO)**

53/94

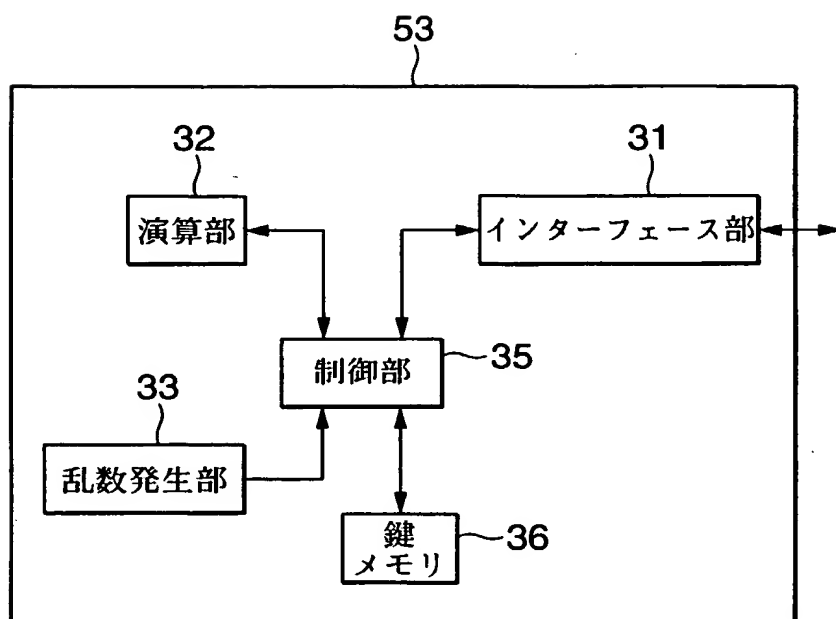


FIG.54

**THIS PAGE BLANK (USPTO)**

54/94

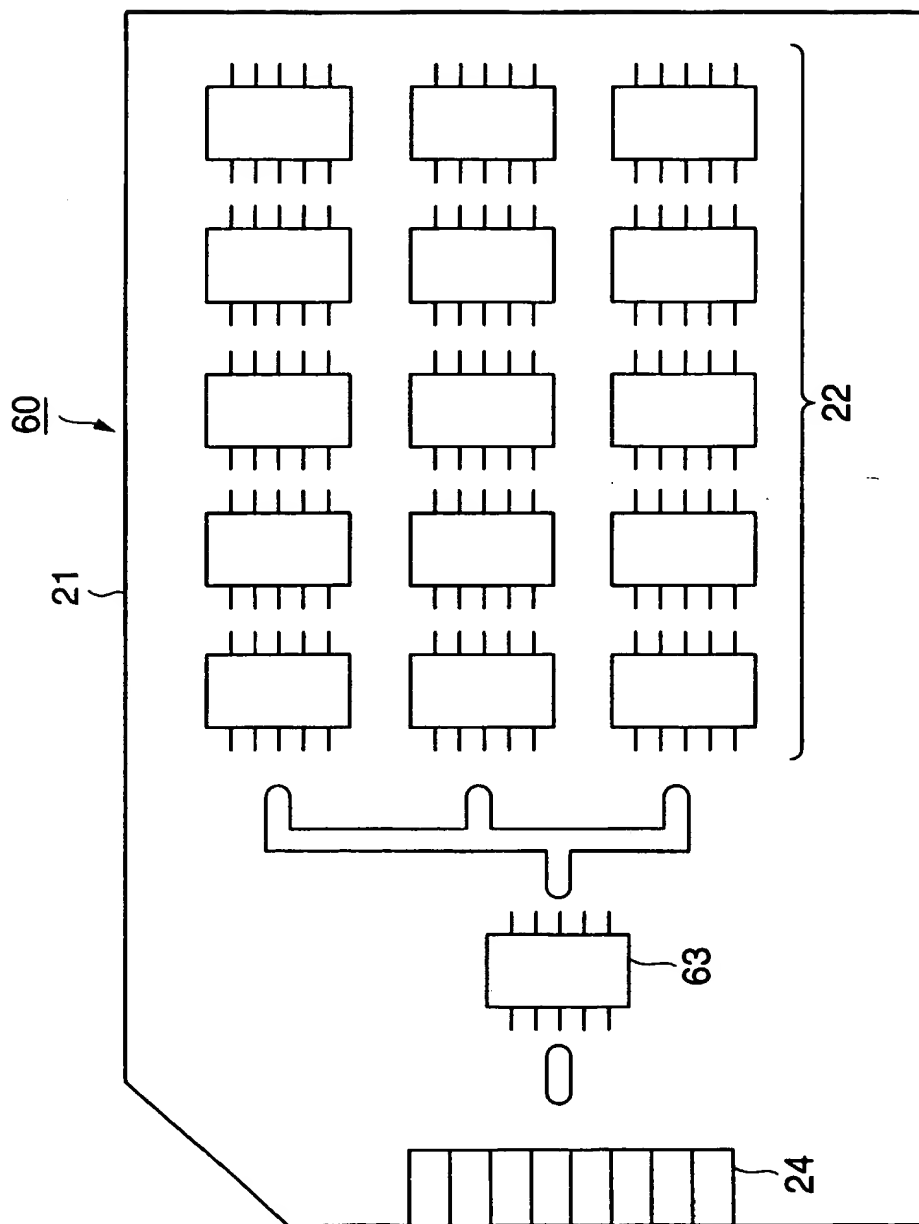


FIG.55

**THIS PAGE BLANK (USPTO)**

55/94

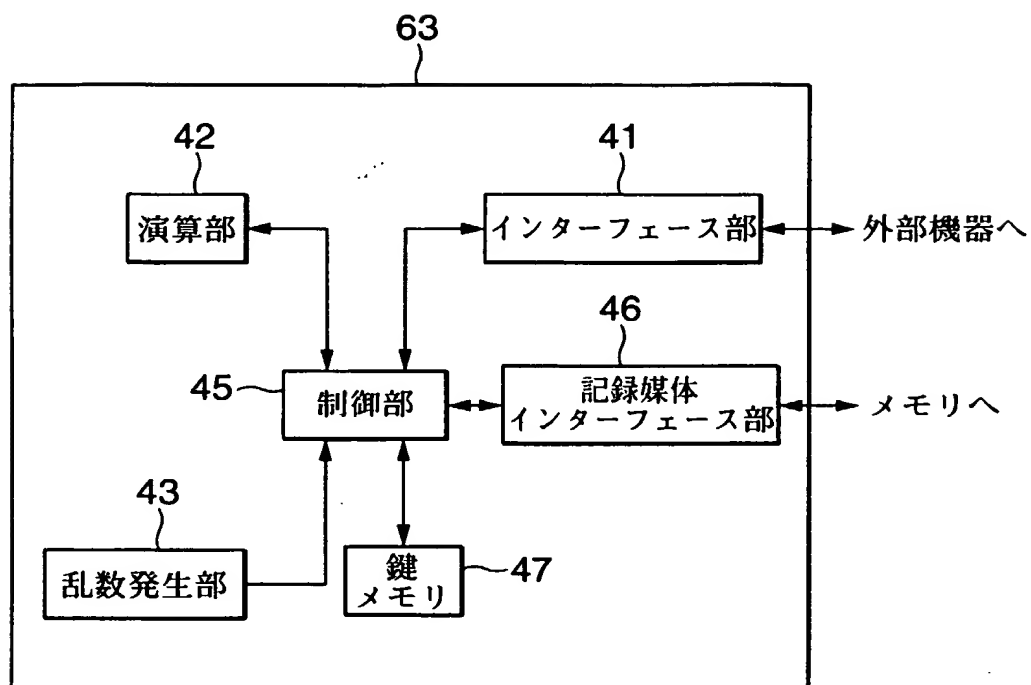
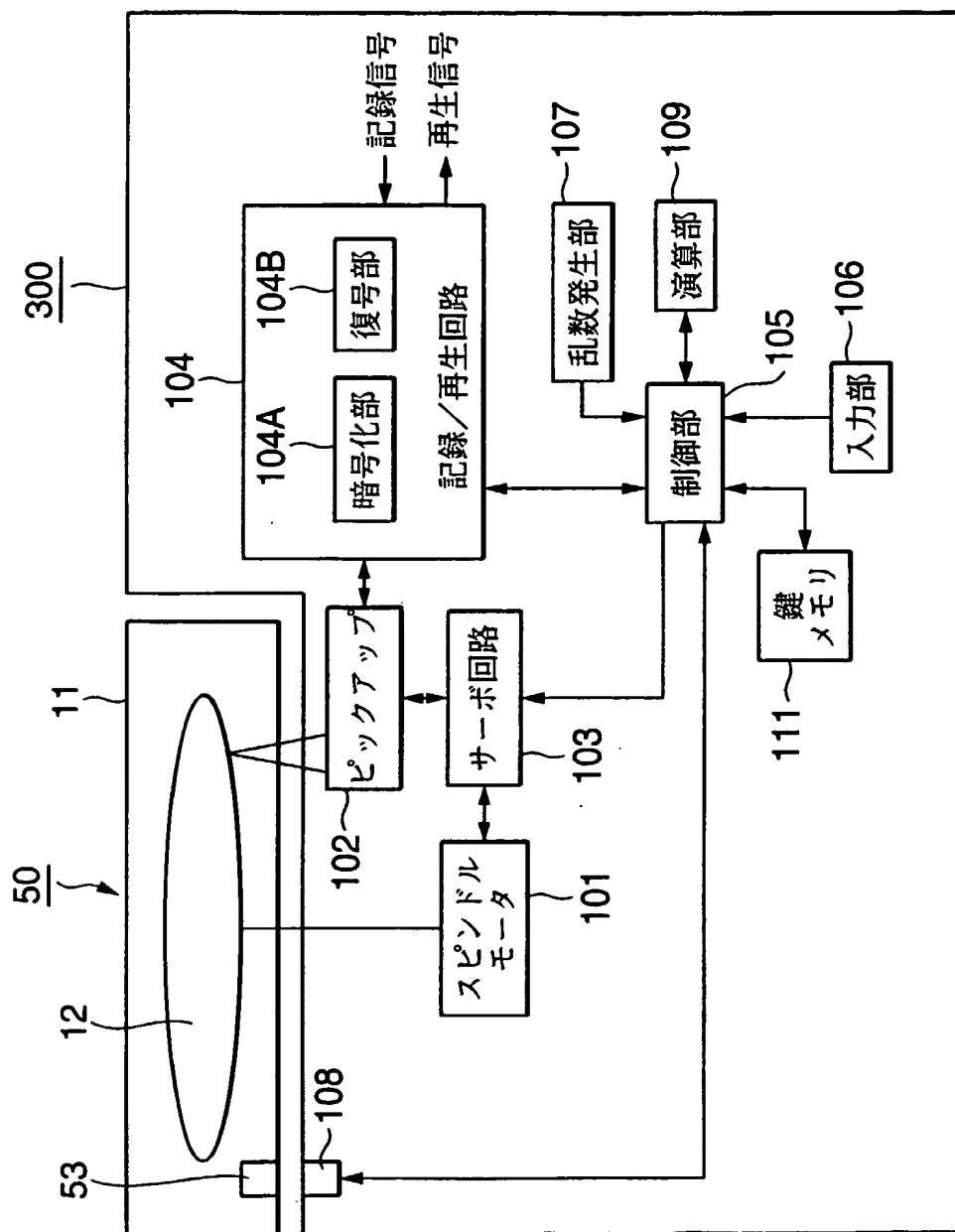


FIG.56

**THIS PAGE BLANK (USPTO)**





**FIG. 57**

**THIS PAGE BLANK (USPTO)**

57/94

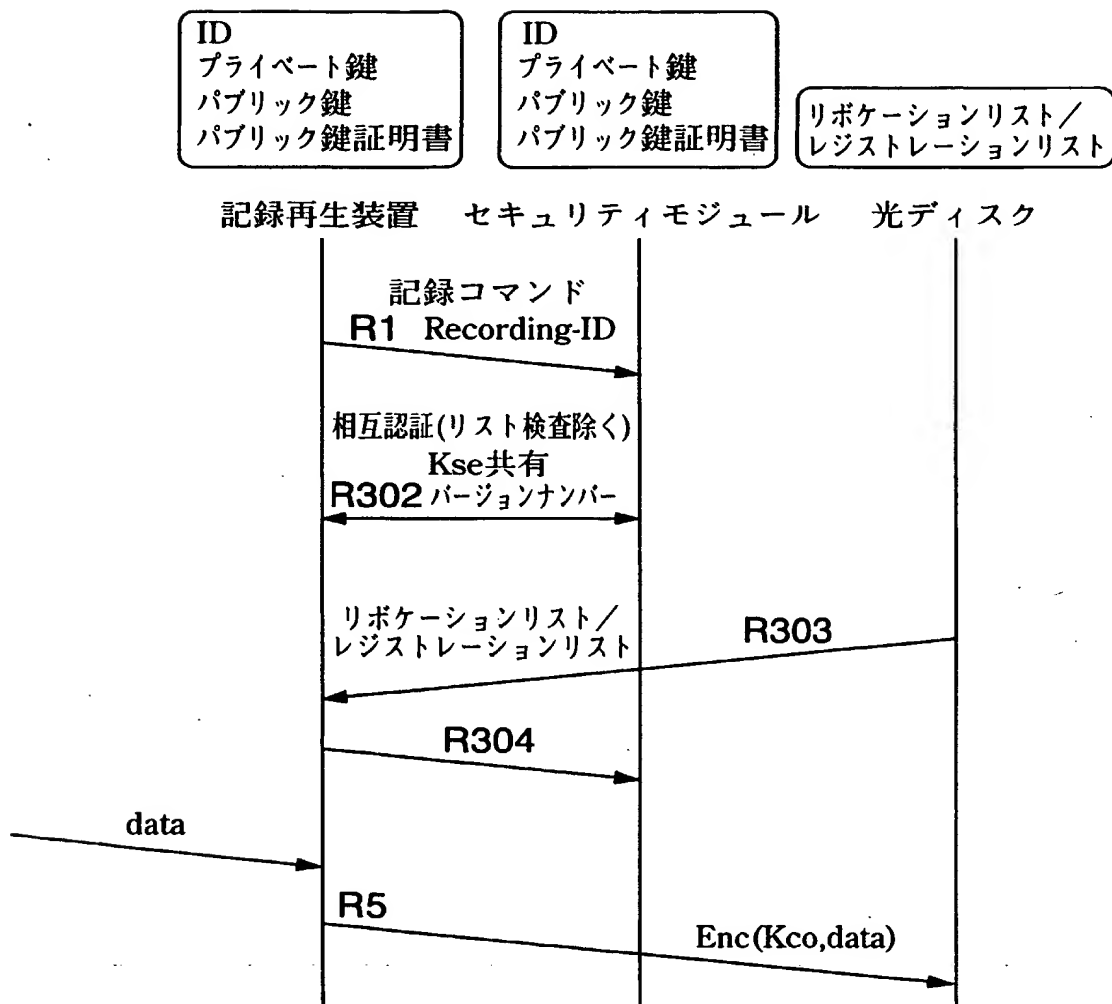


FIG.58

**THIS PAGE BLANK (USPTO)**

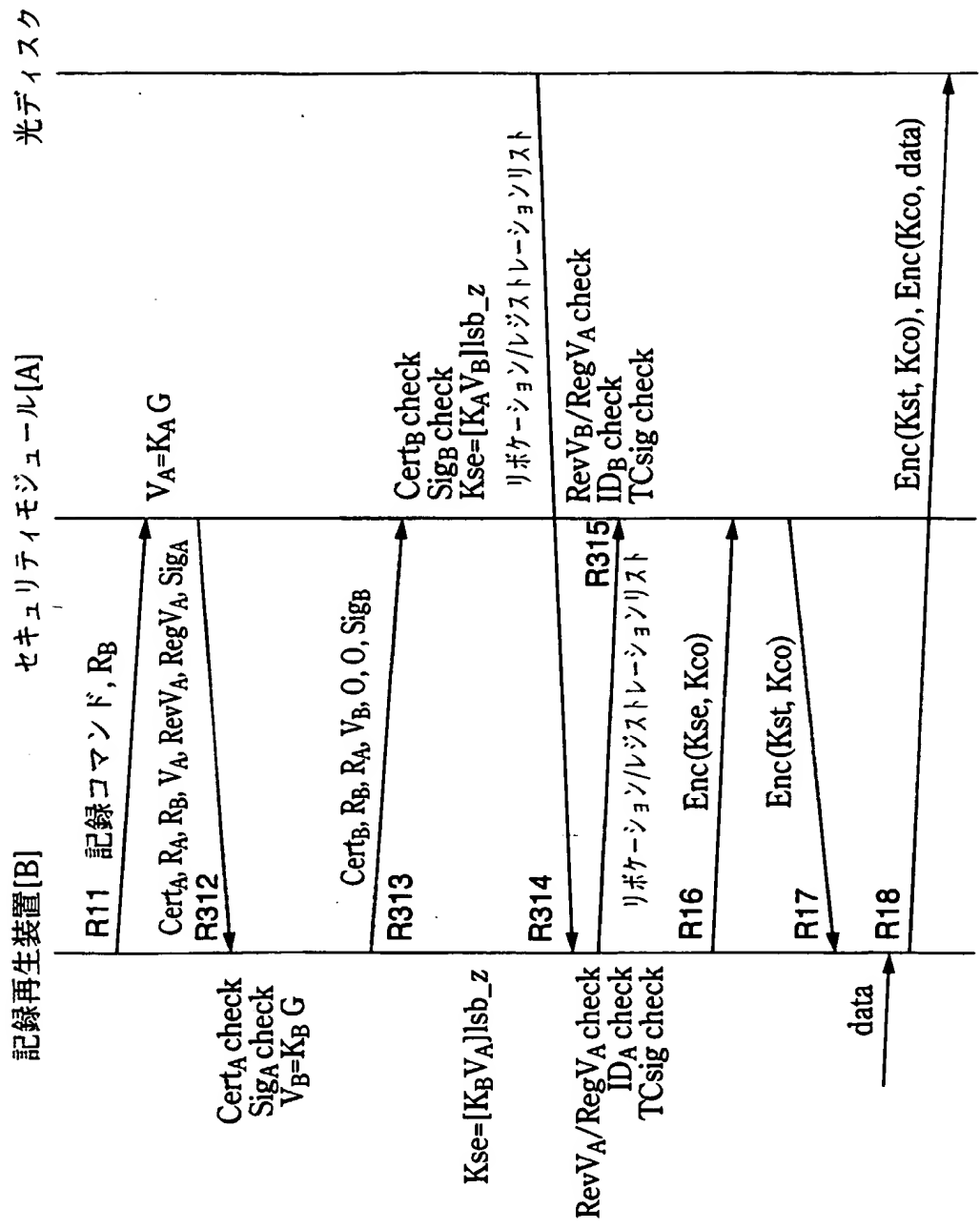


FIG.59

IS PAGE BLANK (USPTO)

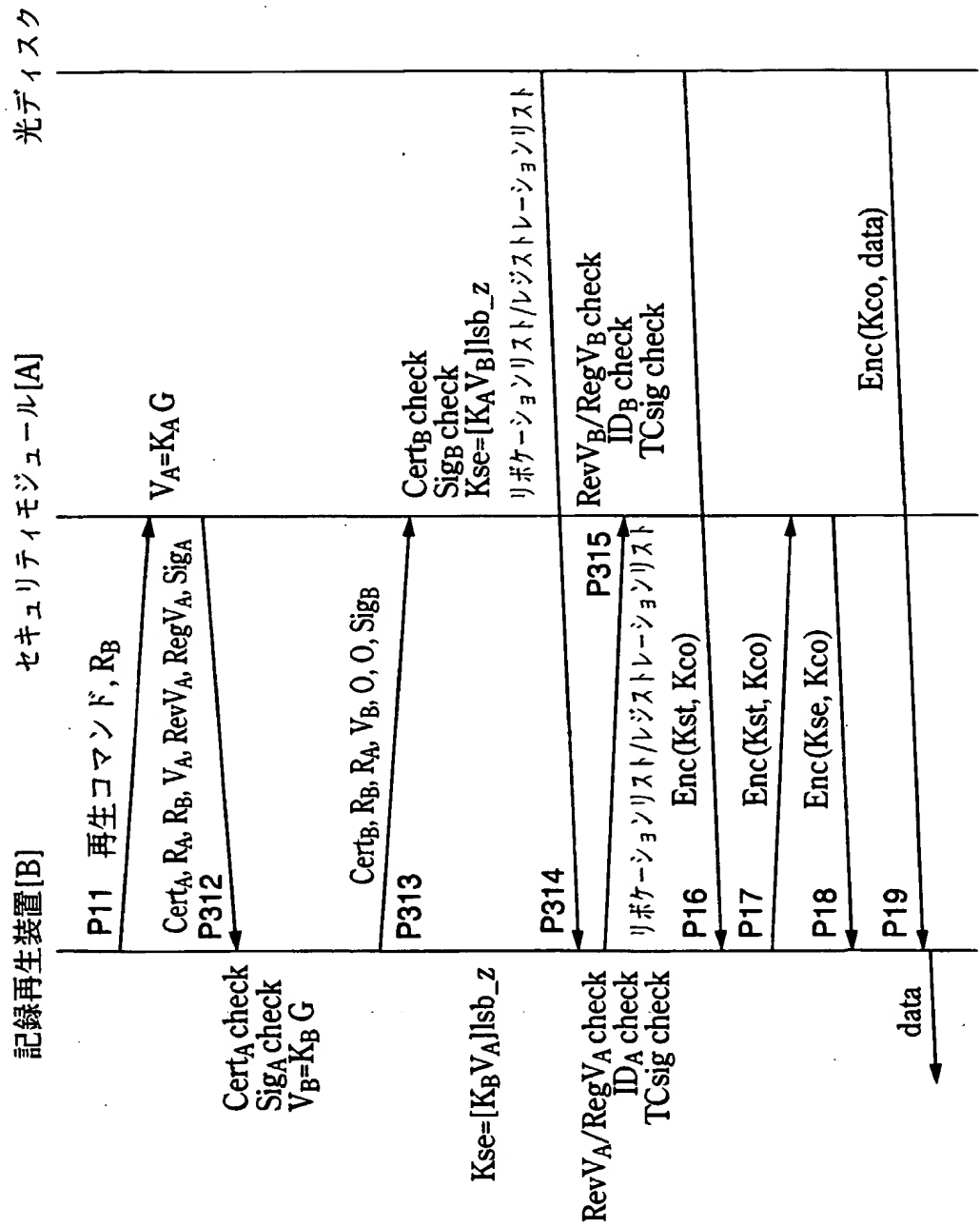


FIG.60

**THIS PAGE BLANK (USPTO)**



60/94

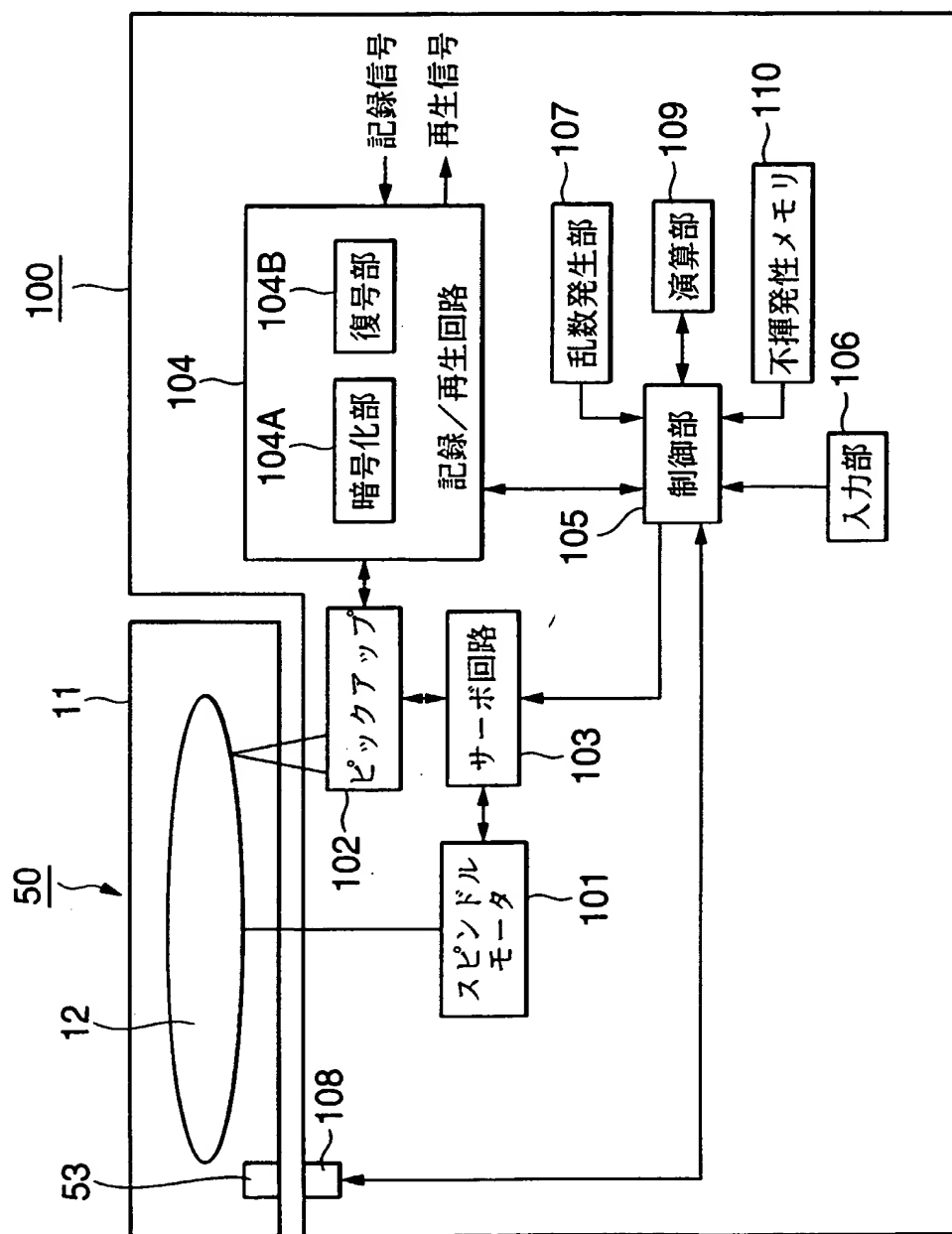


FIG.61

**THIS PAGE BLANK (USPTO)**

61/94

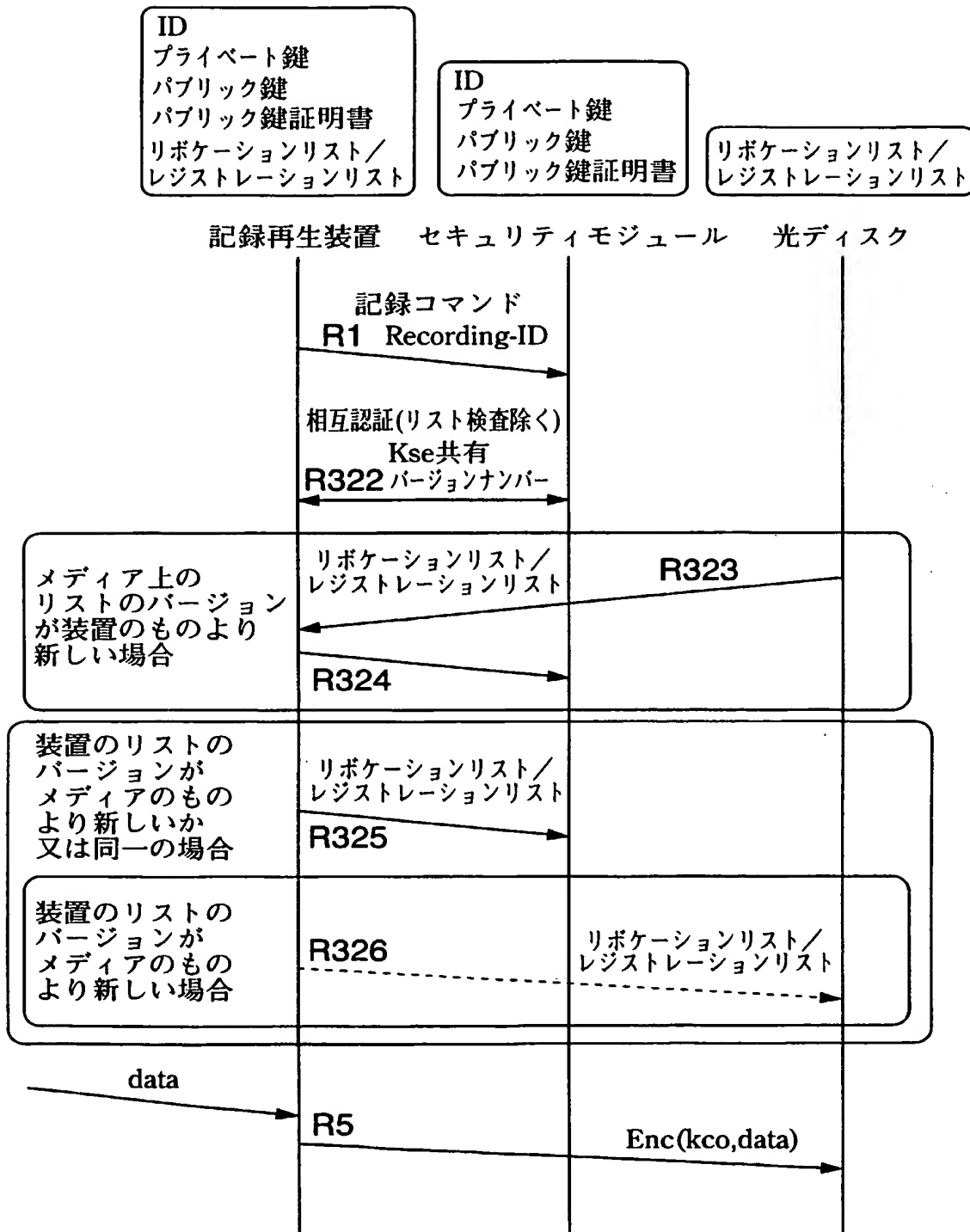


FIG.62

**THIS PAGE BLANK (USPTO)**

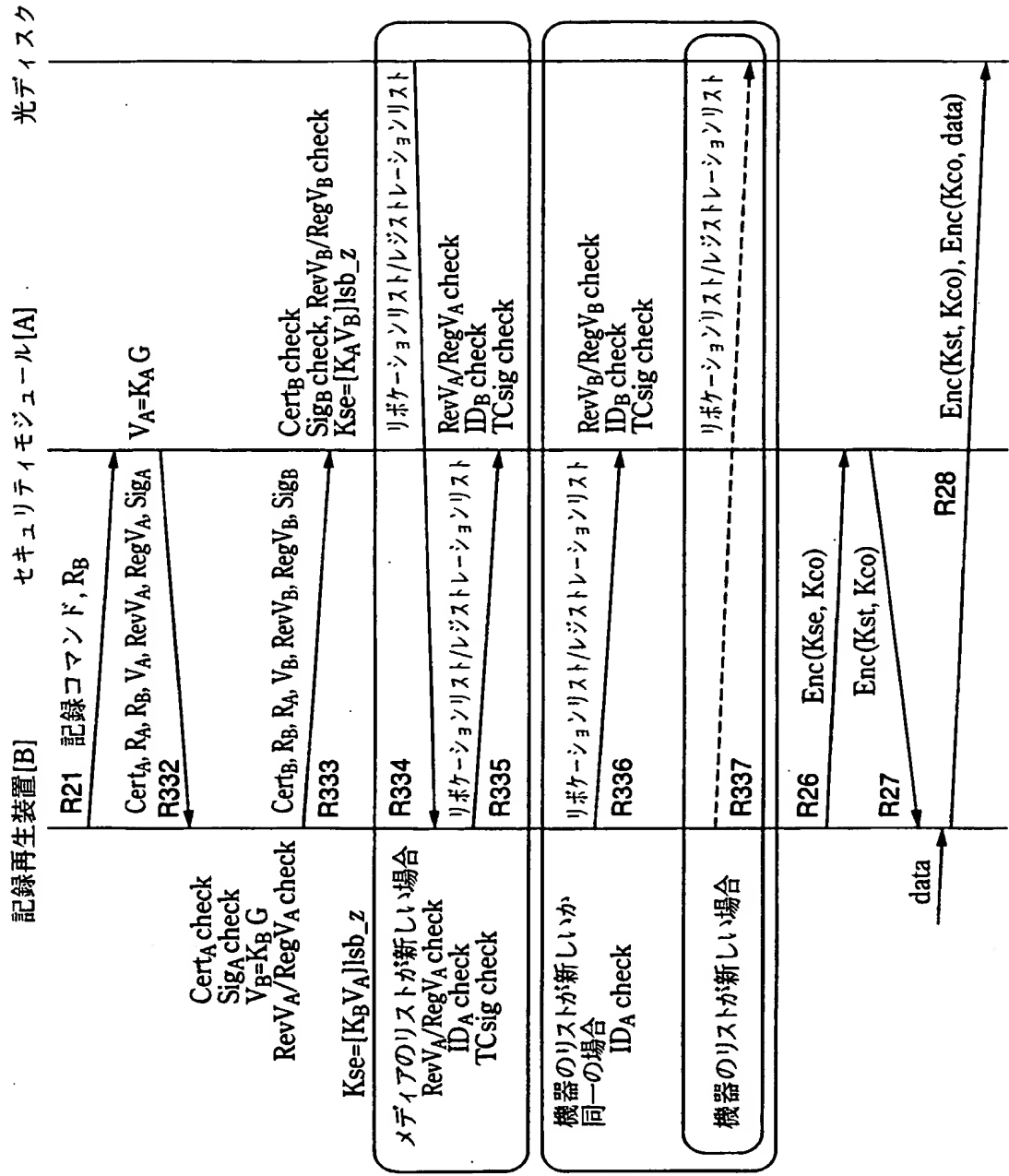


FIG.63

**THIS PAGE BLANK (USPTO)**

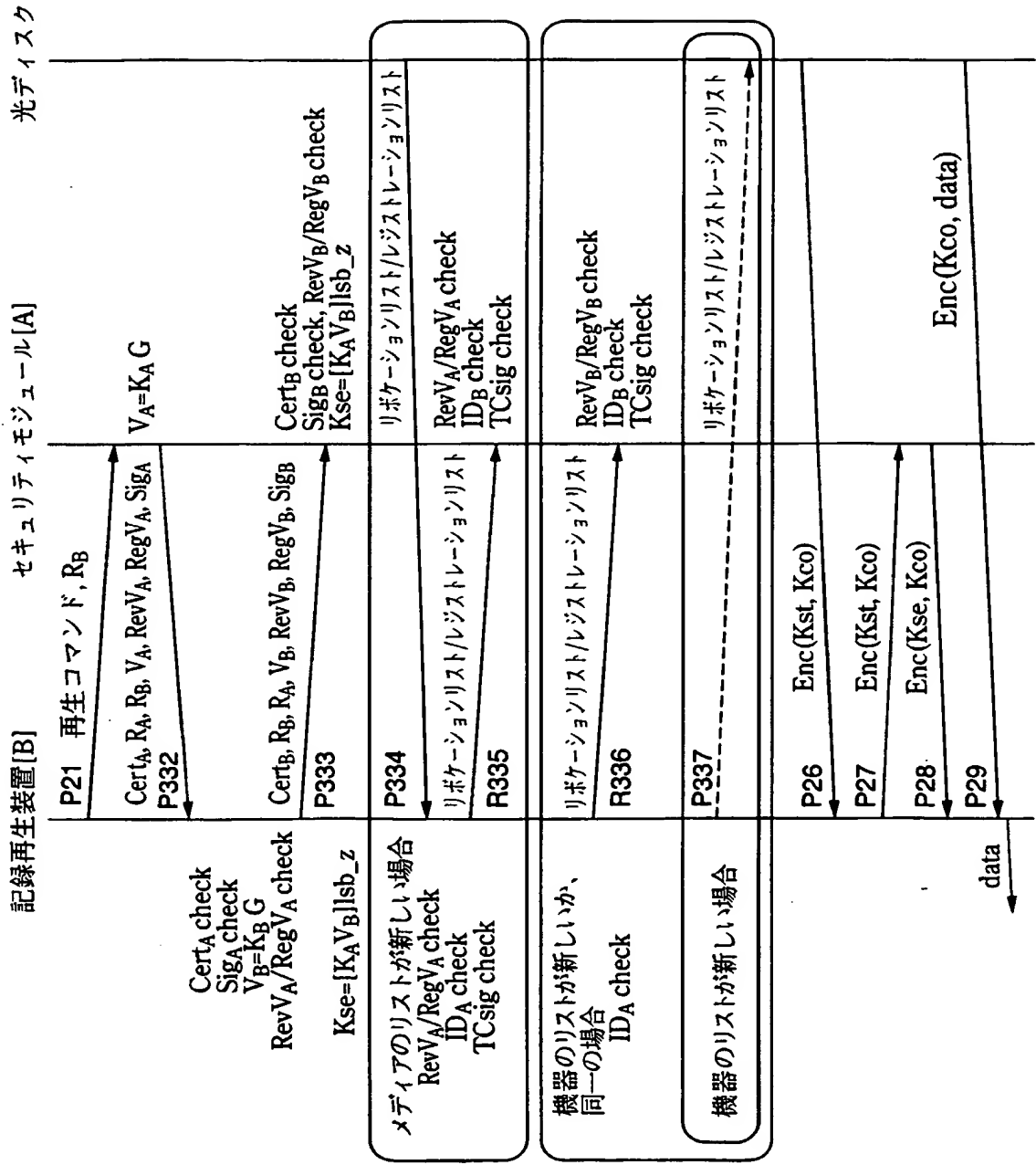
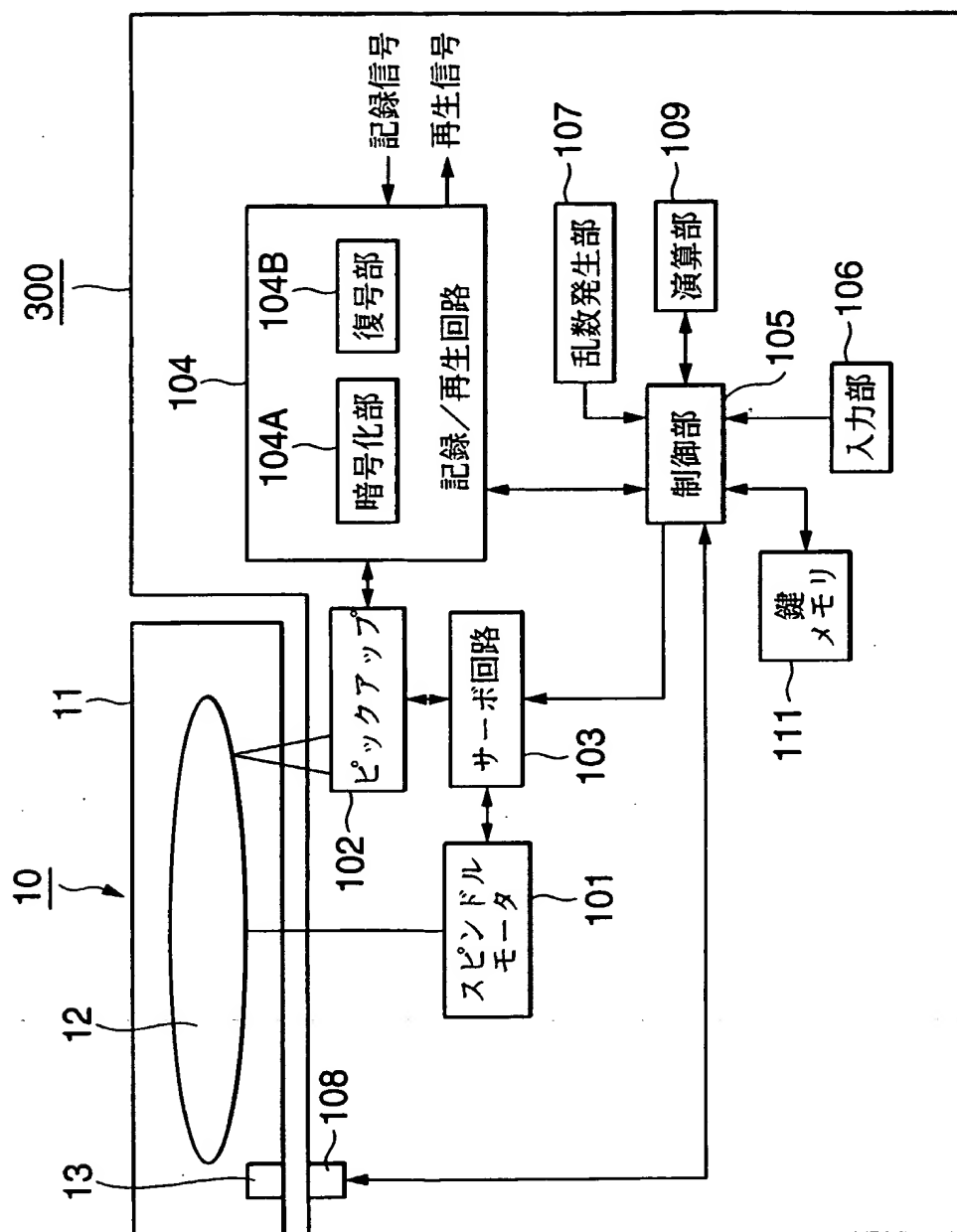


FIG.64

**THIS PAGE BLANK (USPTO)**





**FIG. 65**

**THIS PAGE BLANK (USPTO)**

65/94

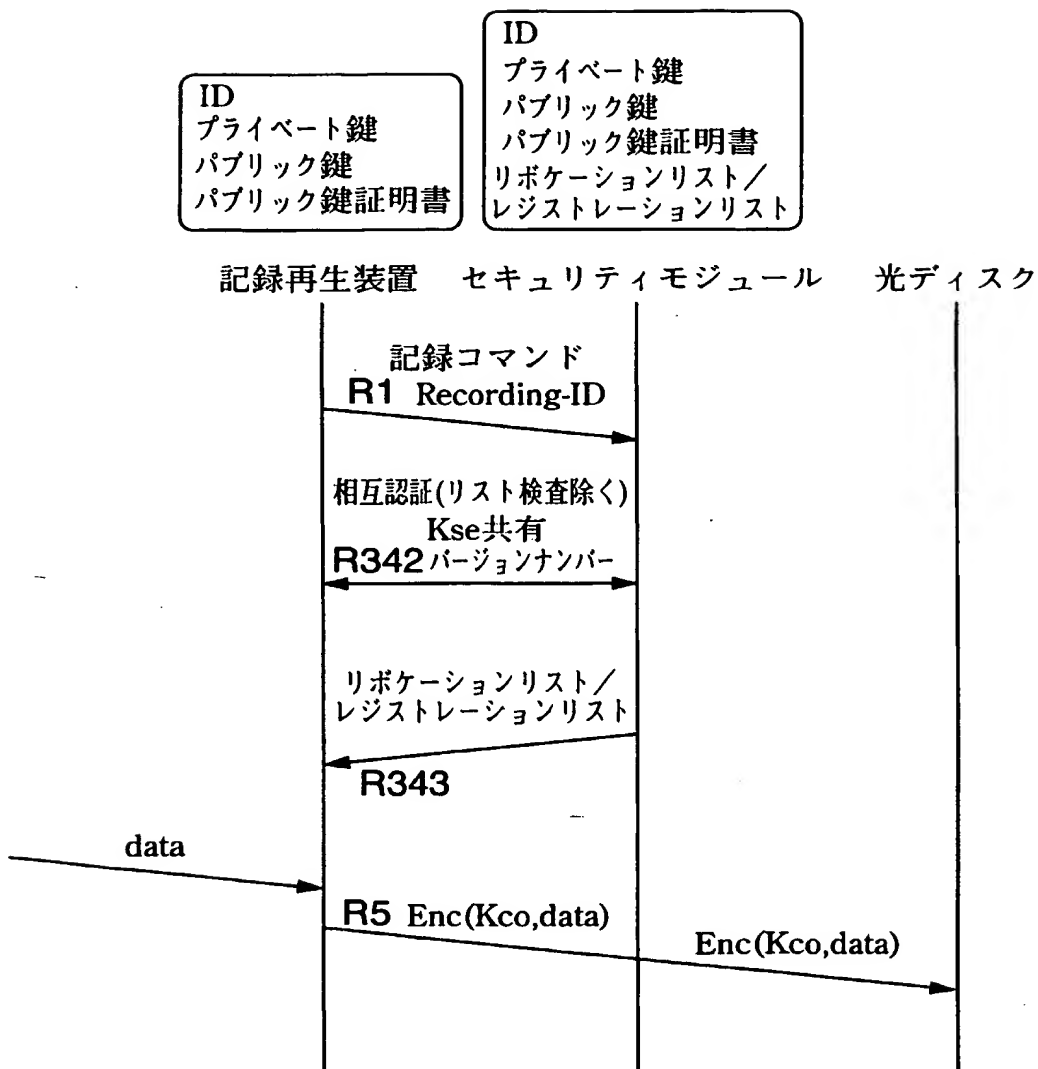


FIG.66

**THIS PAGE BLANK (USPTO)**

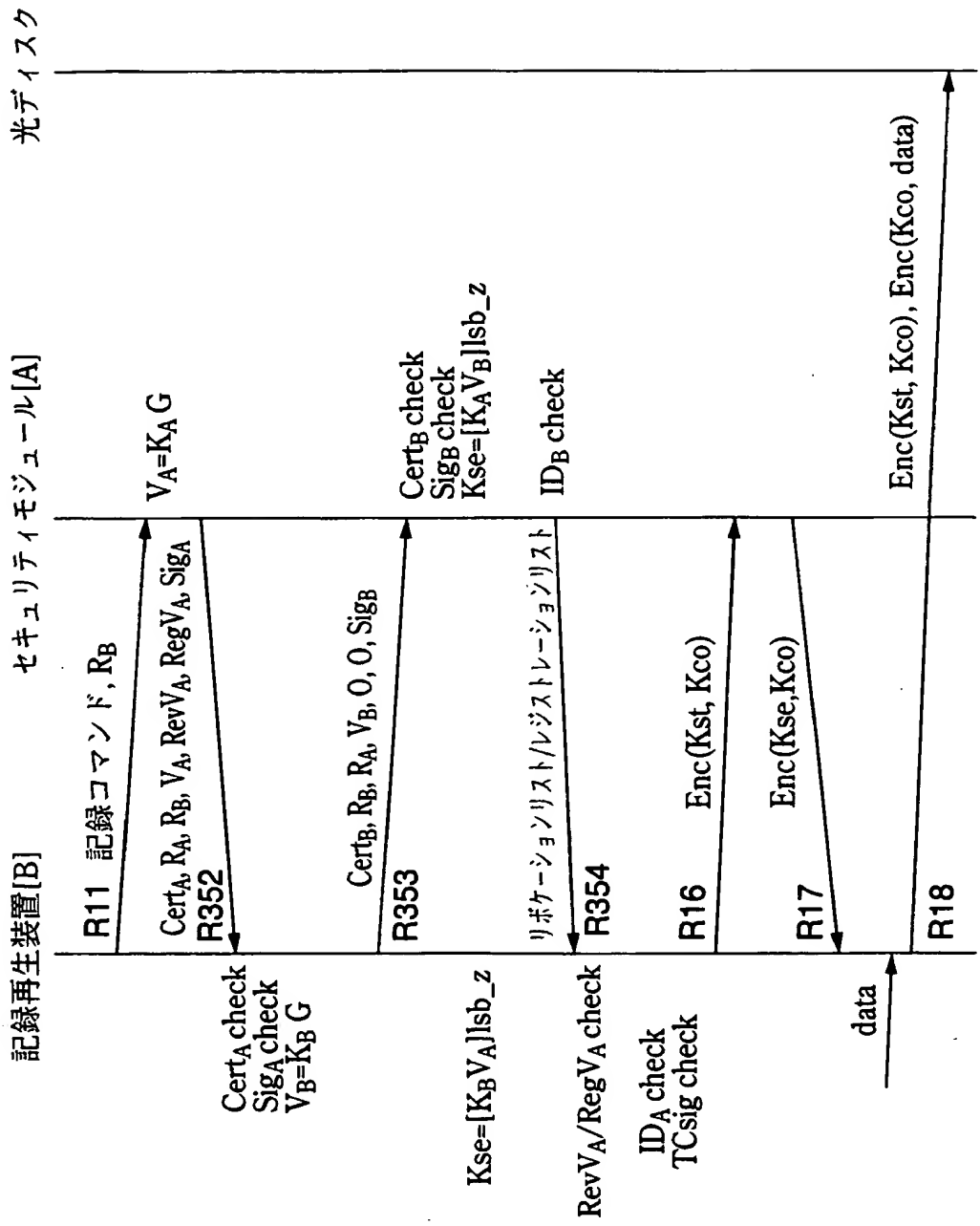


FIG.67

**THIS PAGE BLANK (USPTO)**

67/94

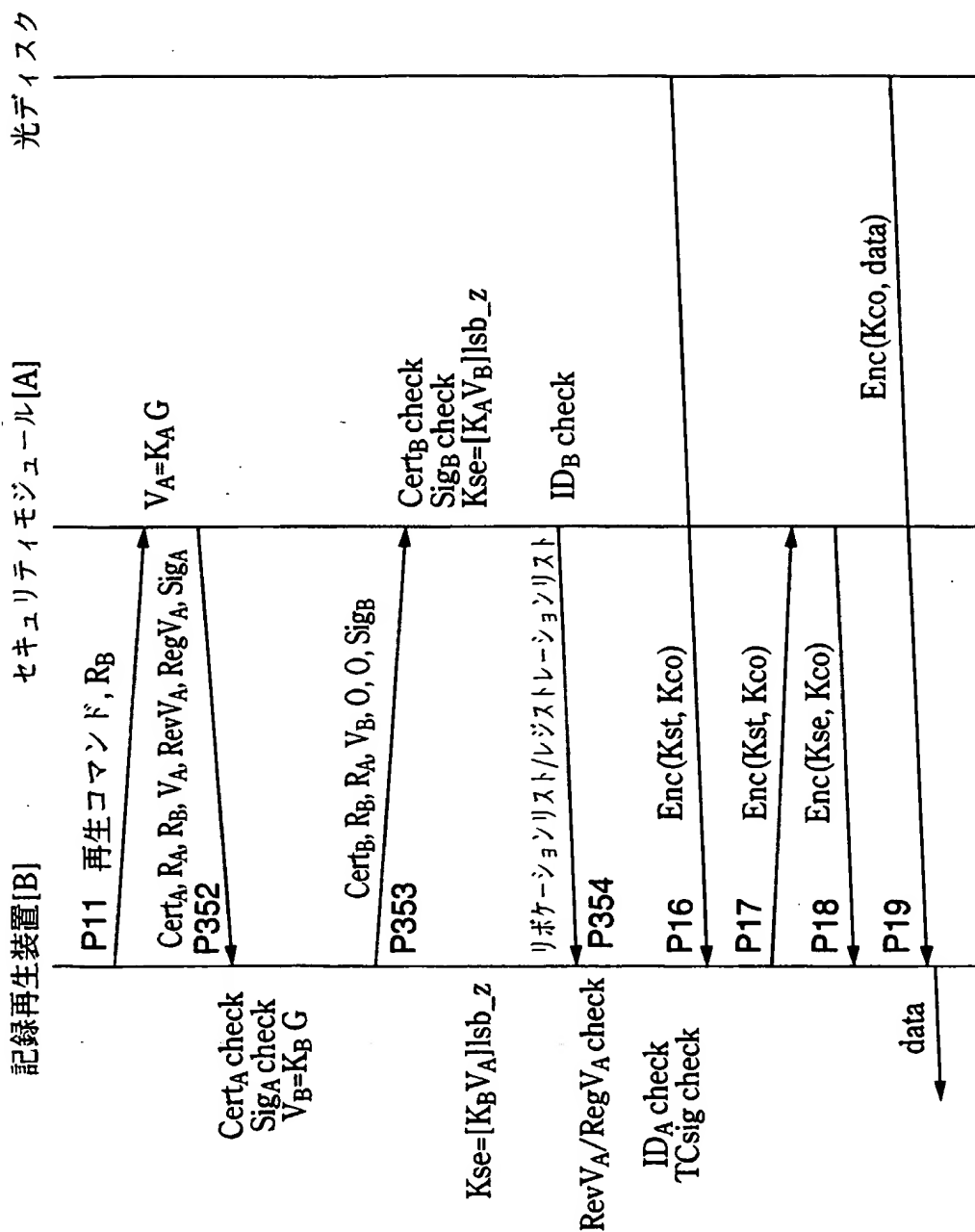


FIG.68

**HIS PAGE BLANK (USPTO)**



68/94

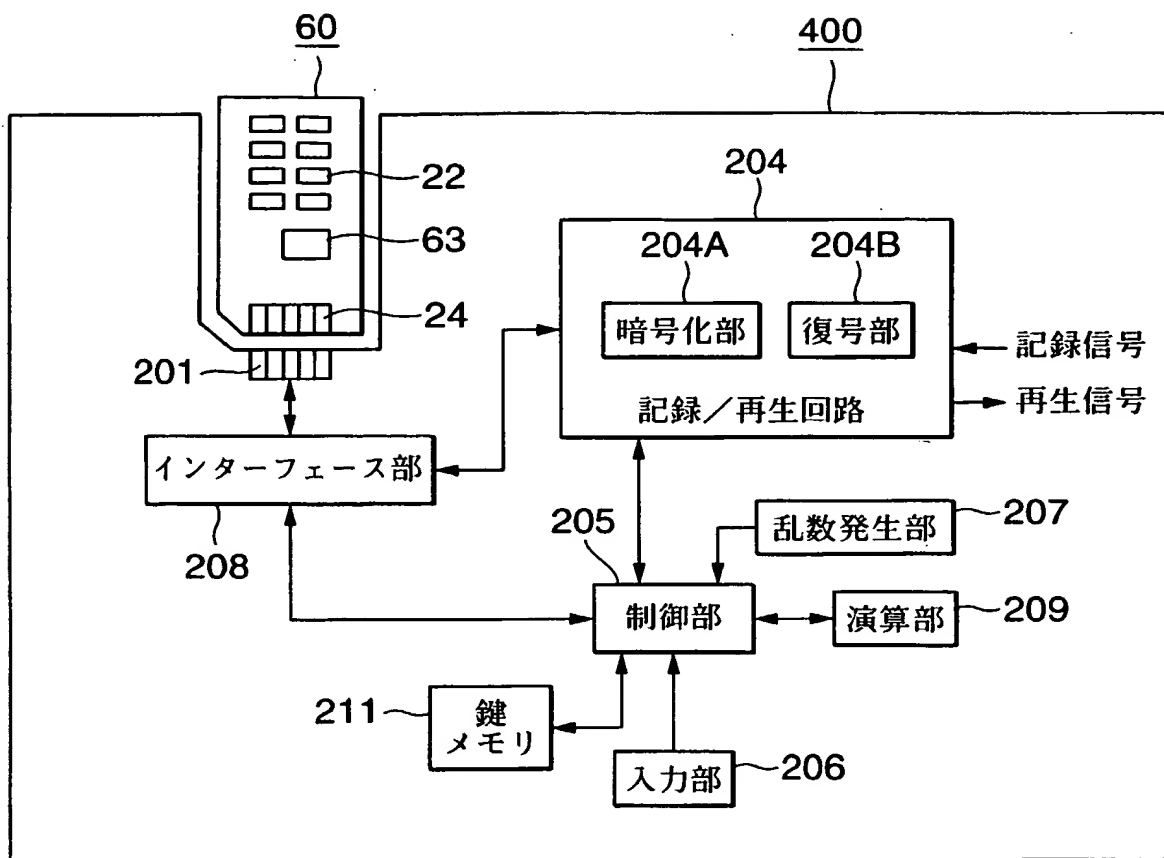


FIG.69

**THIS PAGE BLANK (USPTO)**

69/94

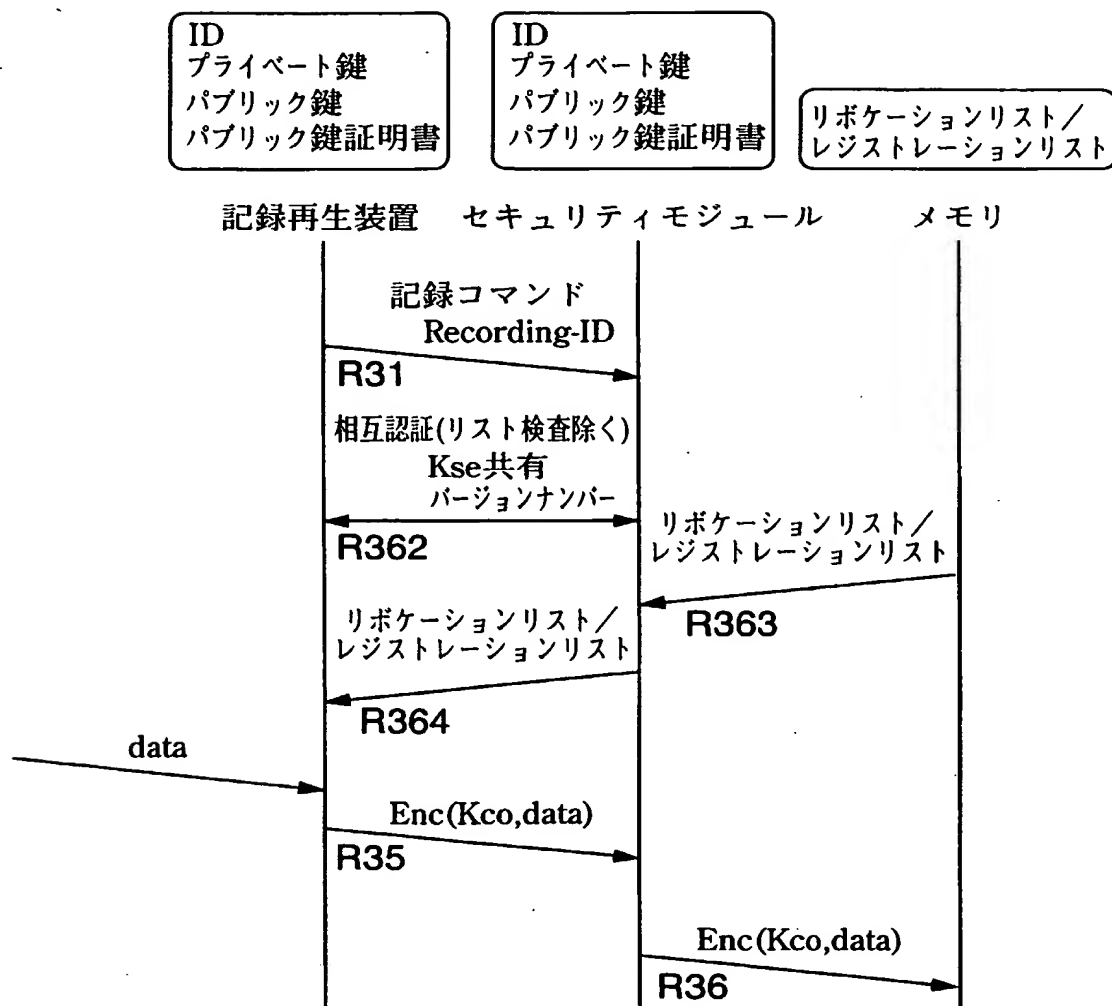


FIG.70

**THIS PAGE BLANK (USPTO)**

70/94

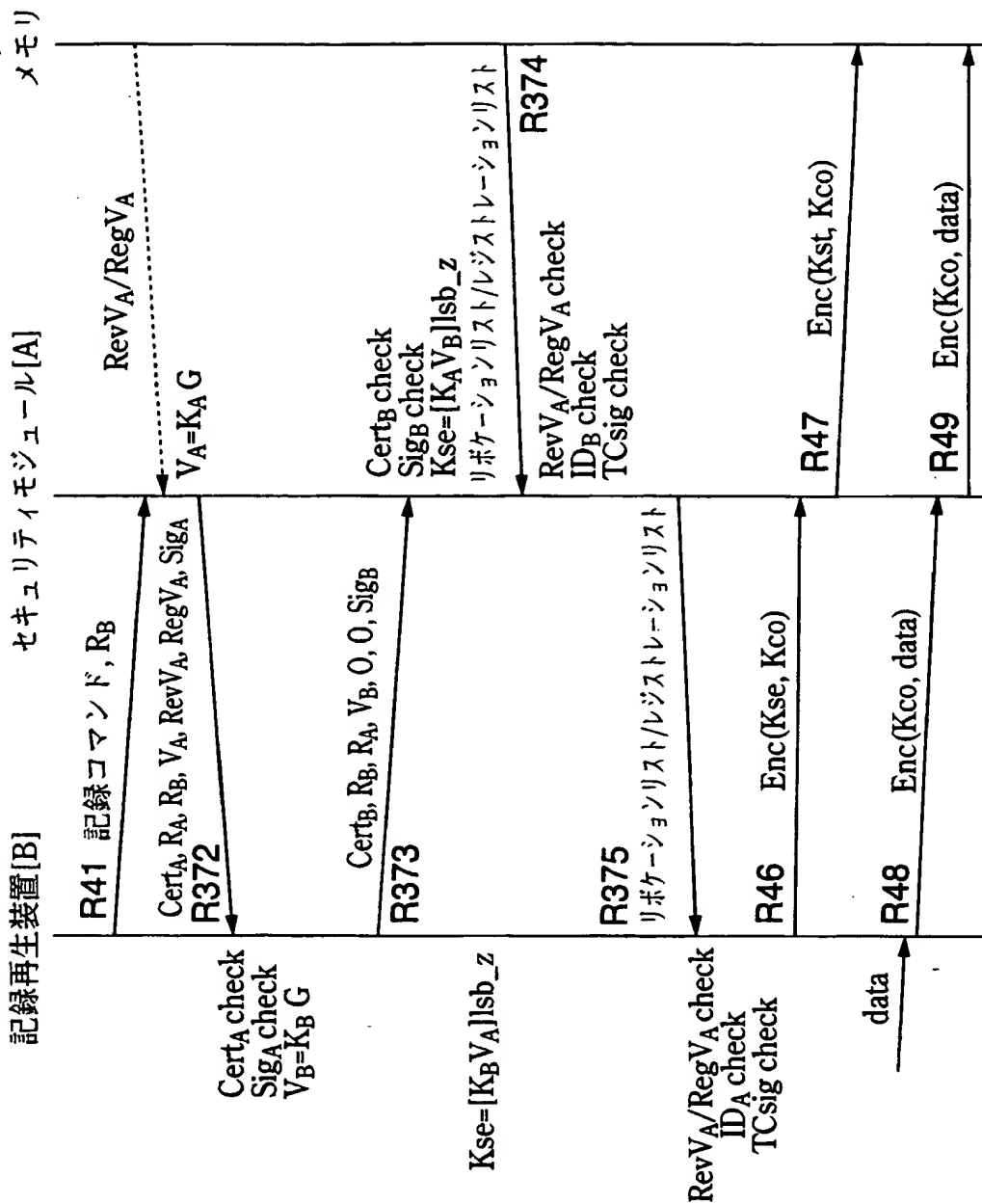


FIG.71

**THIS PAGE BLANK (USPTO)**

71/94

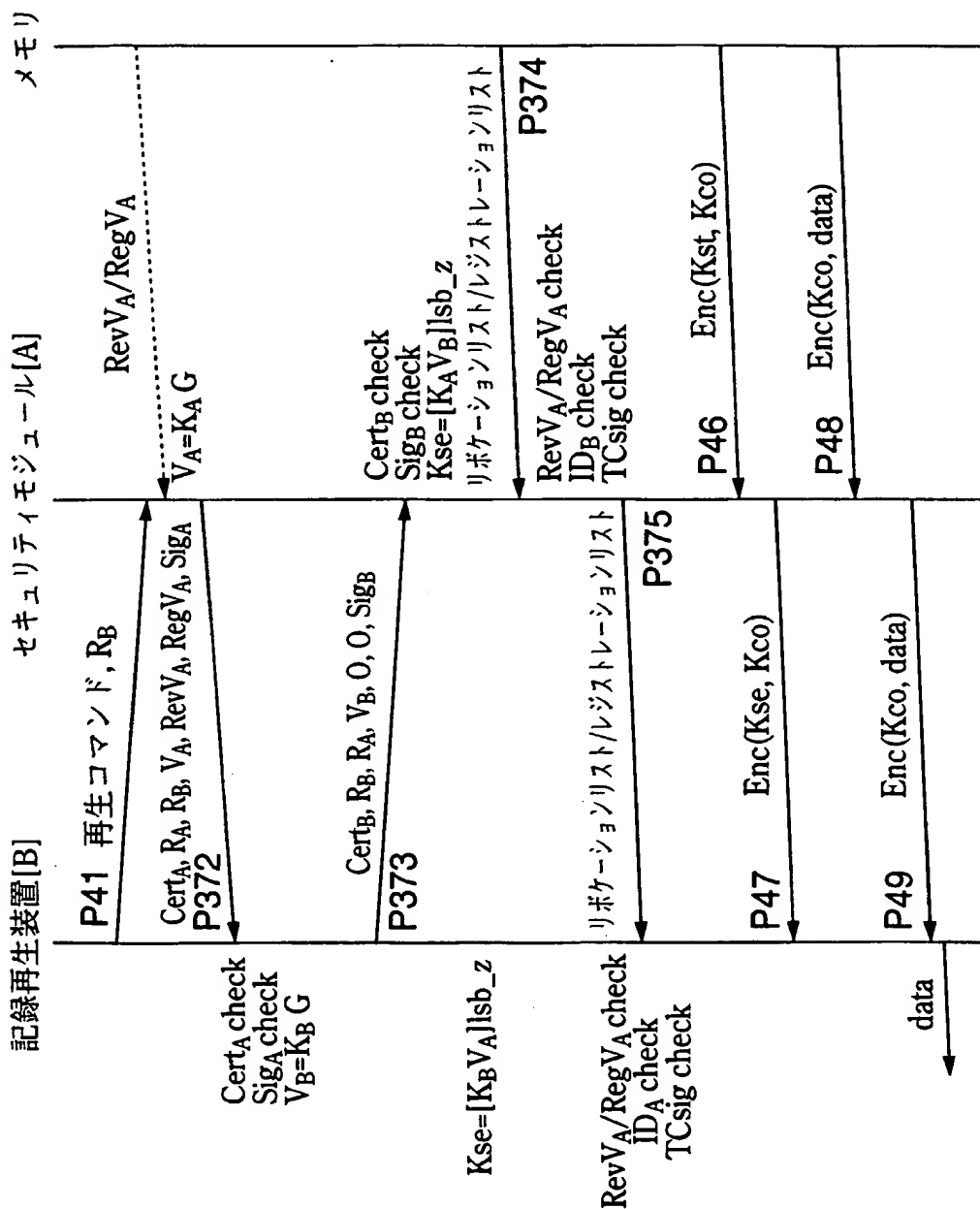


FIG.72

**THIS PAGE BLANK (USPTO)**



72/94

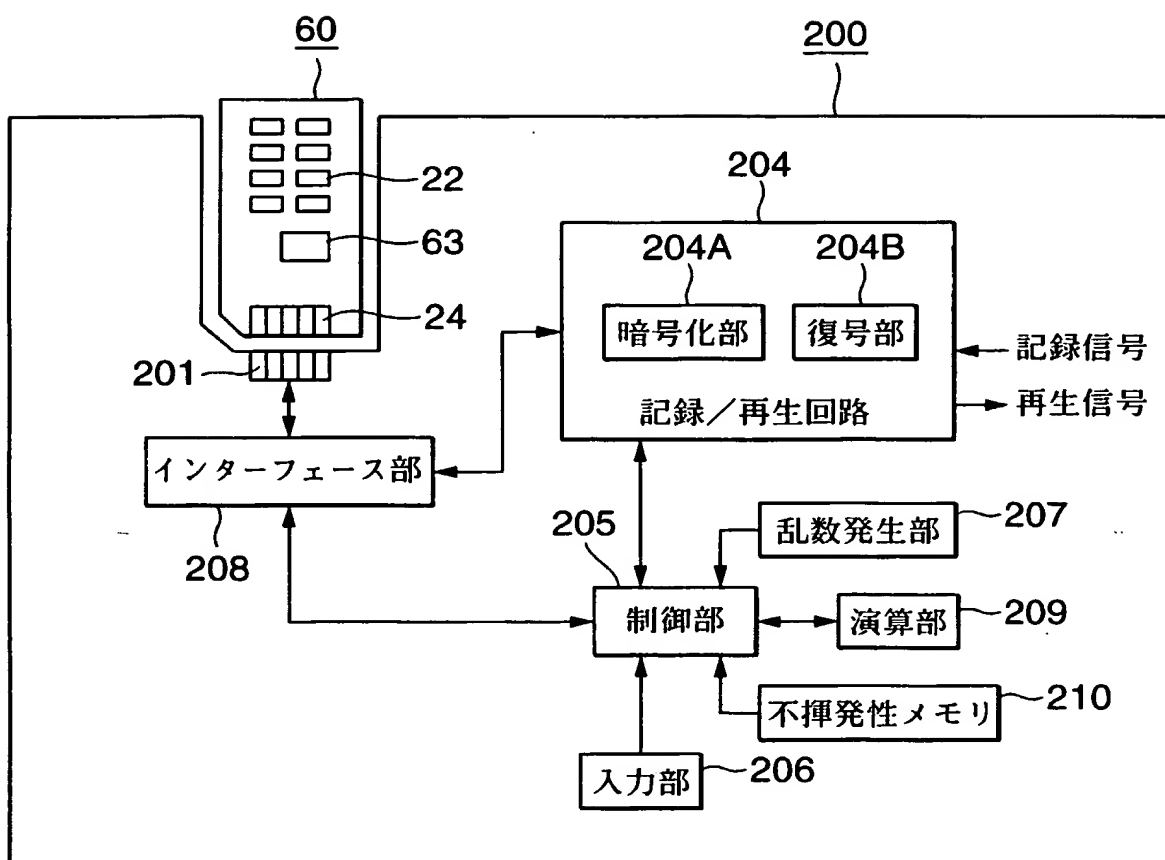


FIG.73

**THIS PAGE BLANK (USPTO)**

73/94

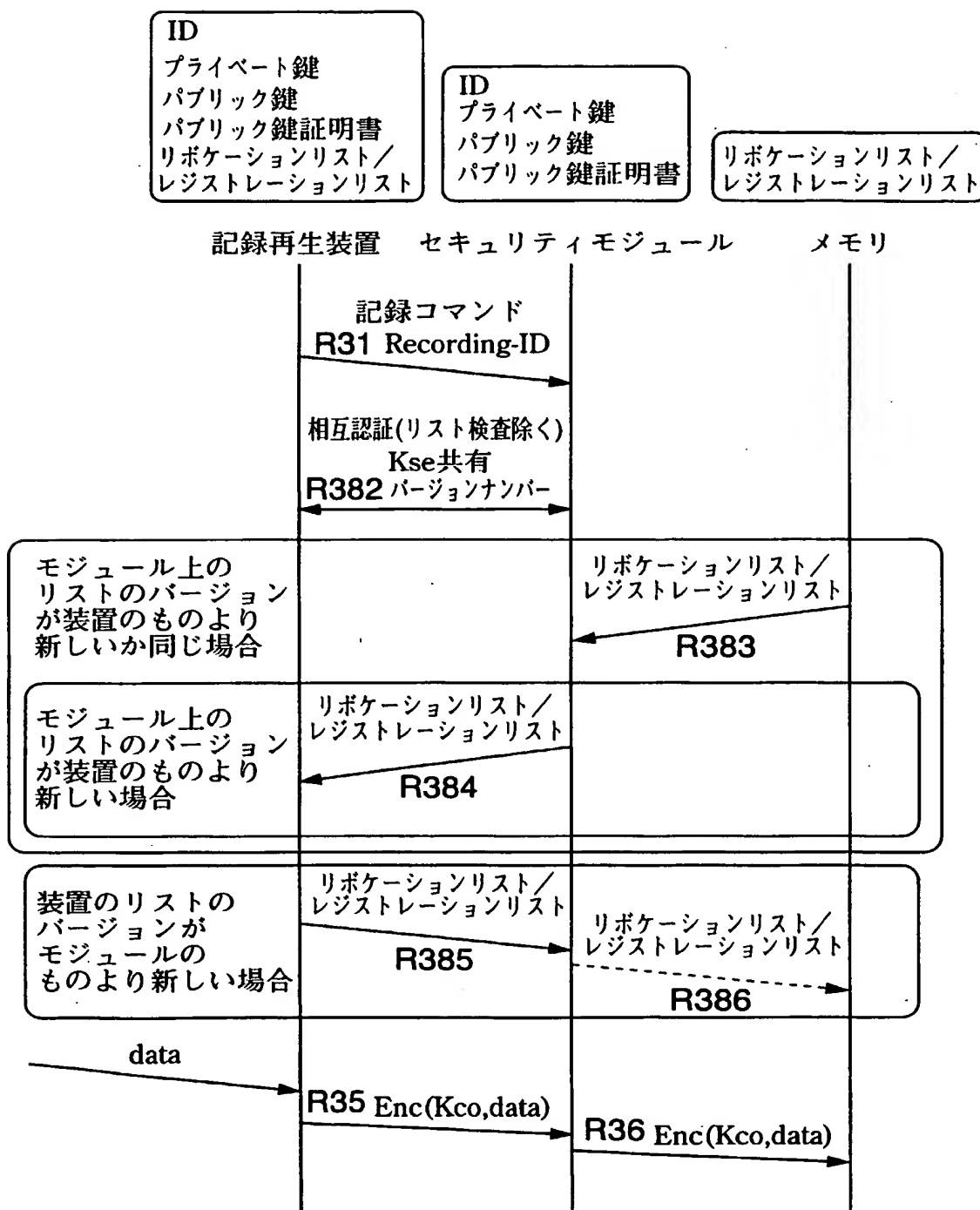


FIG.74

**THIS PAGE BLANK (USPTO)**

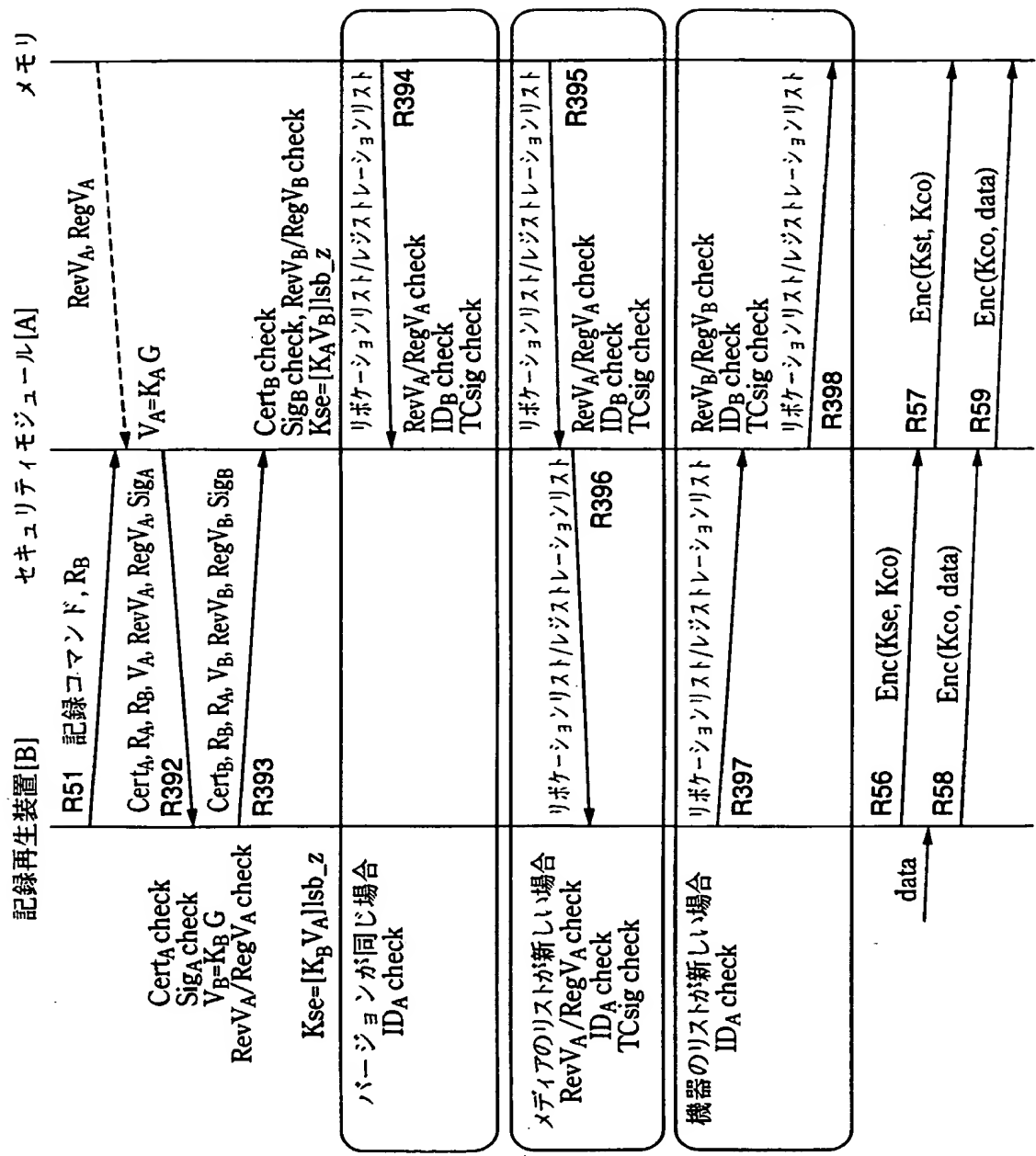


FIG.75

**THIS PAGE BLANK (USPTO)**

75/94

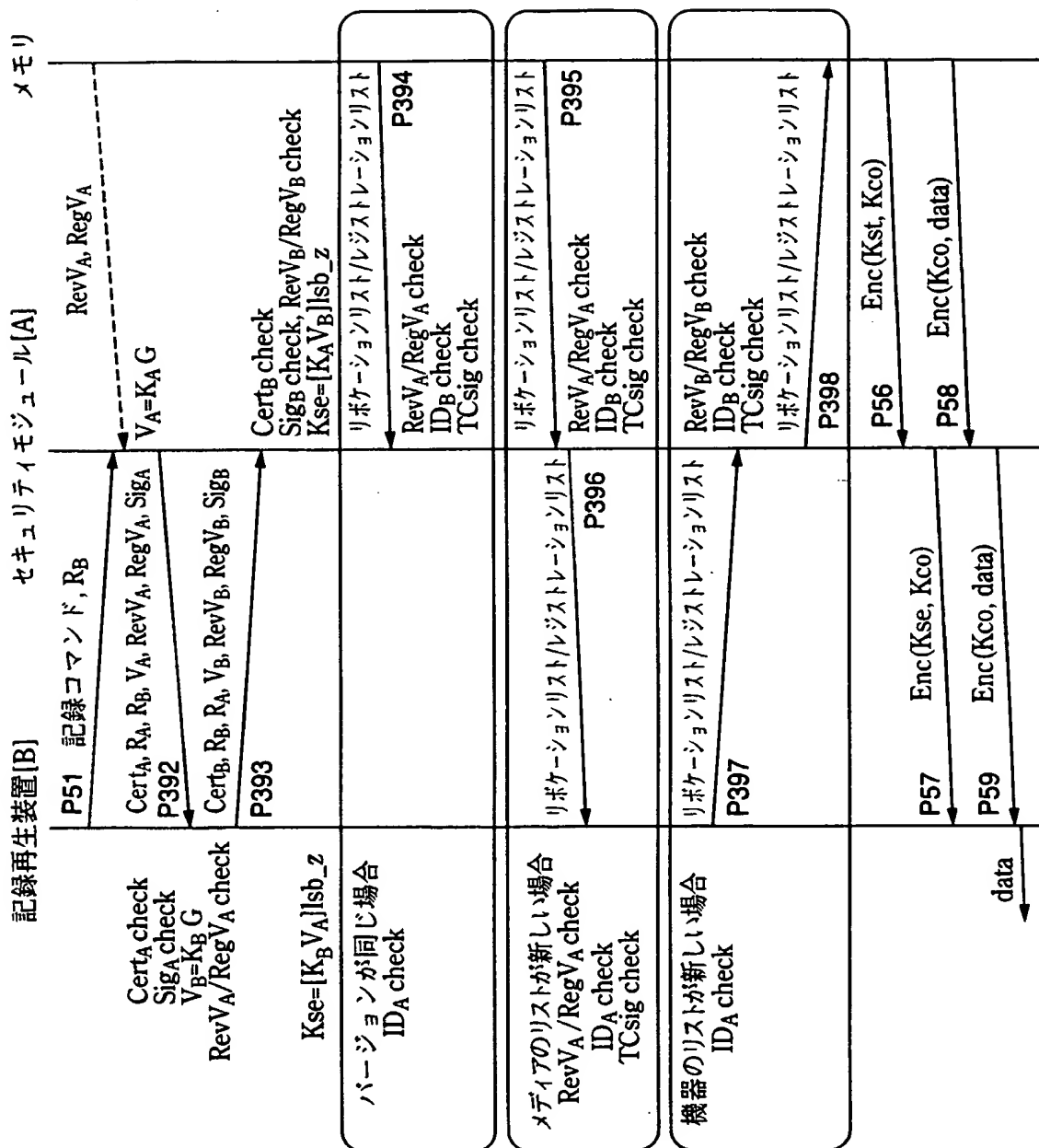


FIG.76

**THIS PAGE BLANK (USPTO)**



76/94

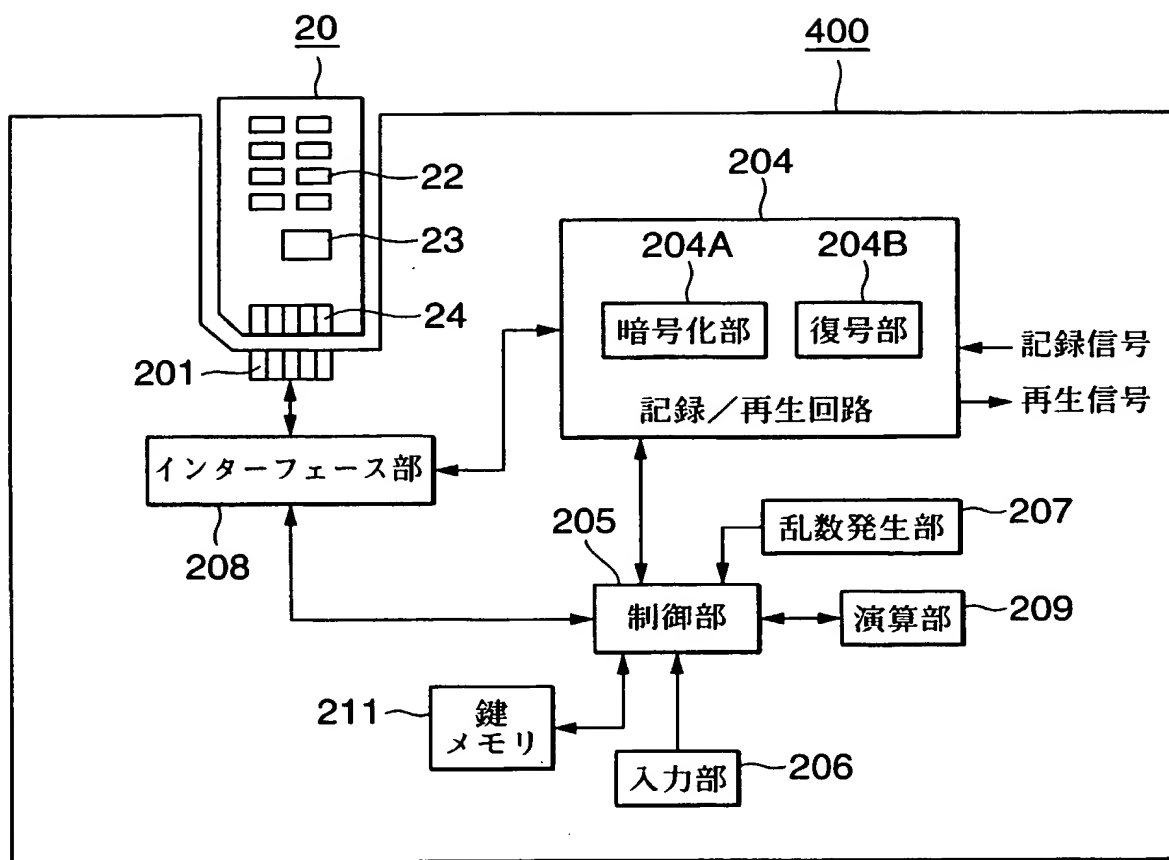


FIG.77

**THIS PAGE BLANK (USPTO)**

77/94

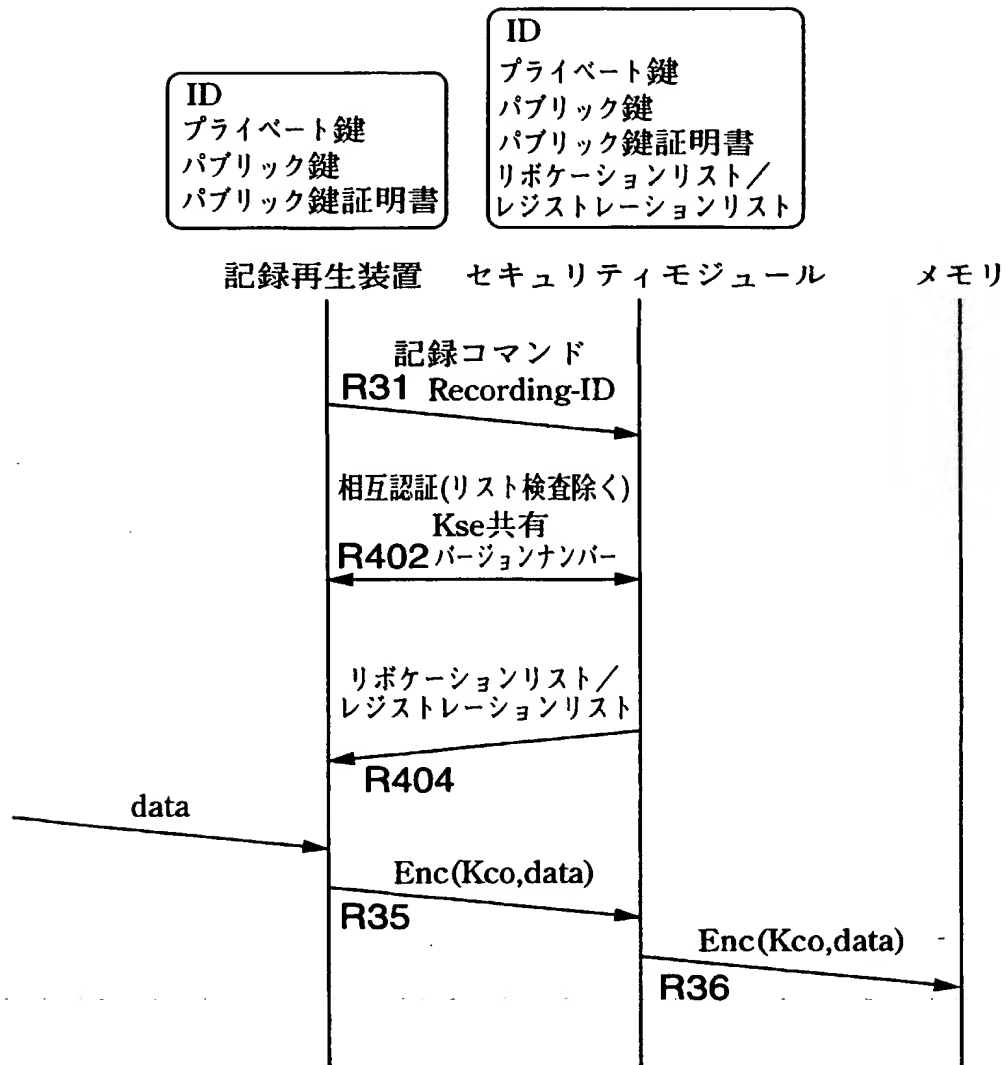


FIG.78

**THIS PAGE BLANK (USPTO)**

78/94

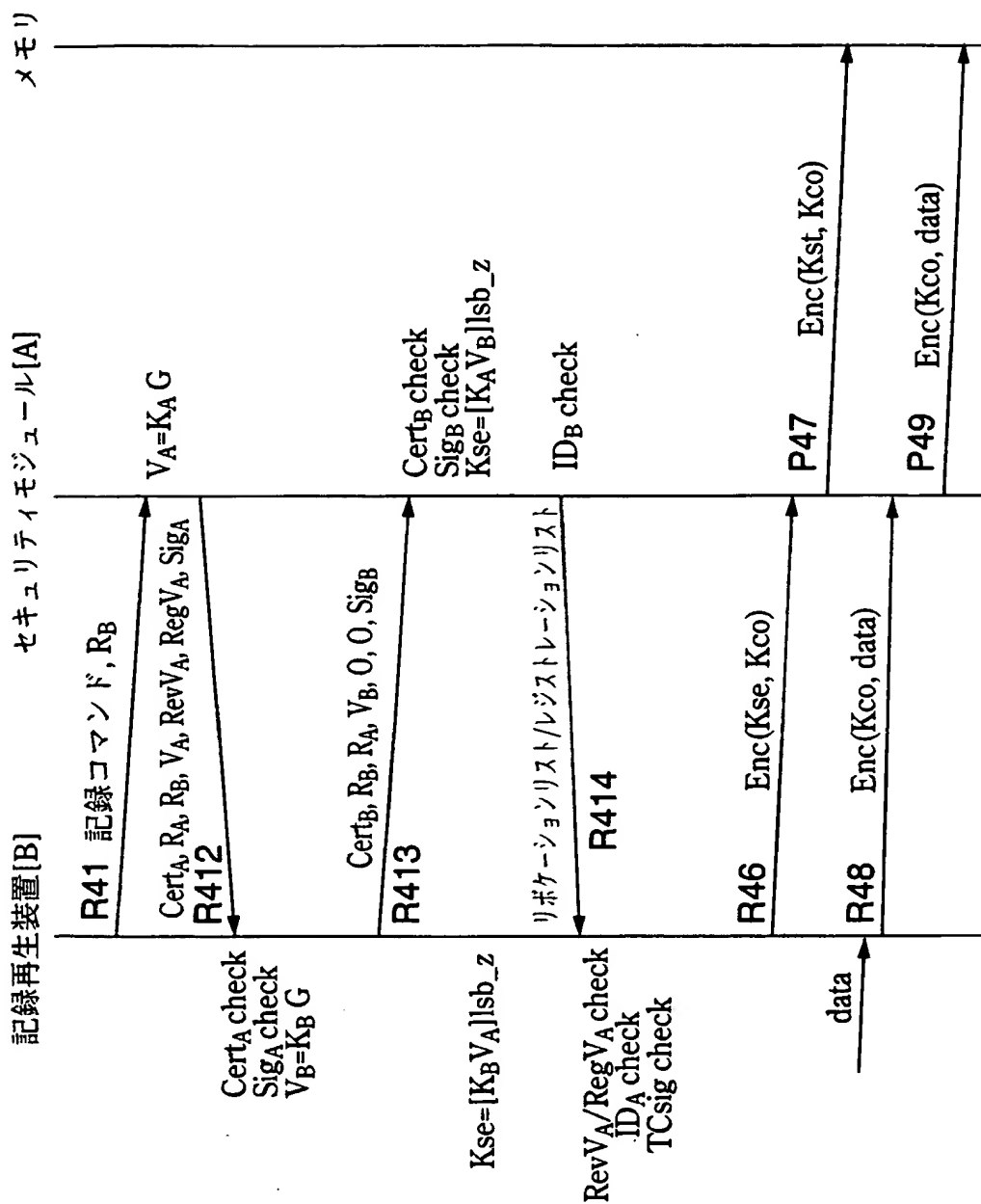


FIG.79

**THIS PAGE BLANK (USPTO)**

79/94

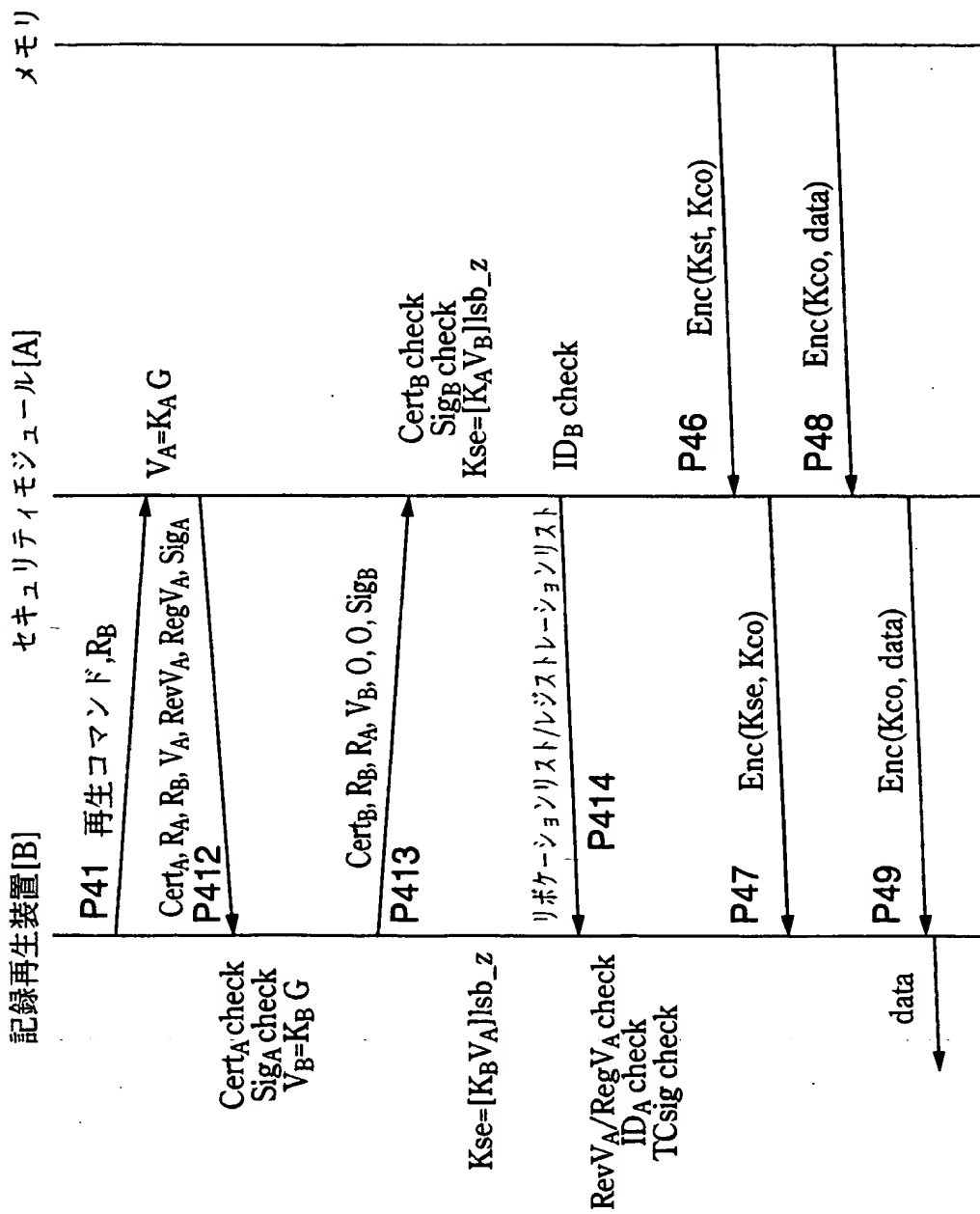


FIG.80

**THIS PAGE BLANK (USPTO)**



80/94

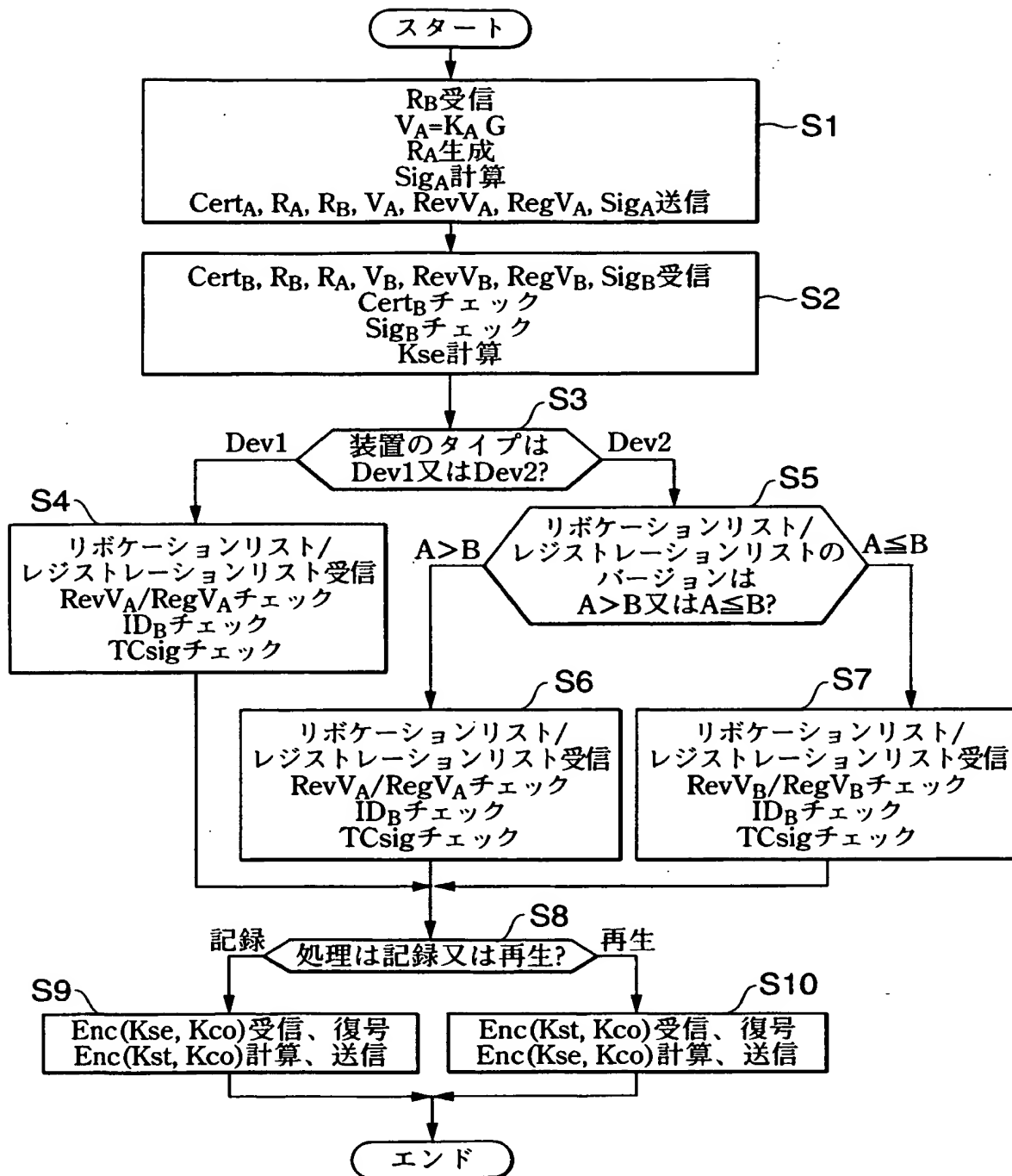


FIG.81

**THIS PAGE BLANK (USPTO)**

81/94

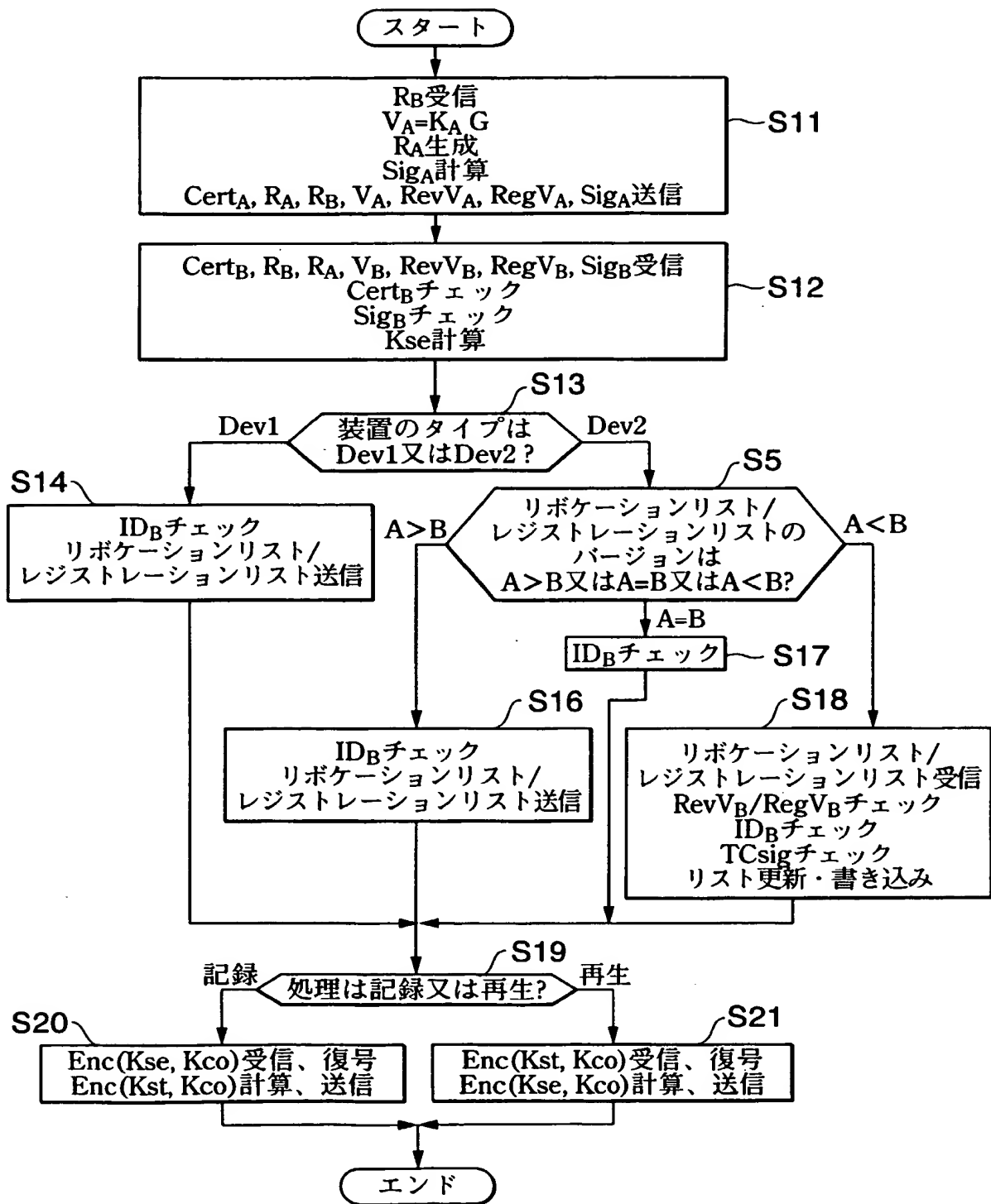


FIG.82

**THIS PAGE BLANK (USPTO)**

82/94

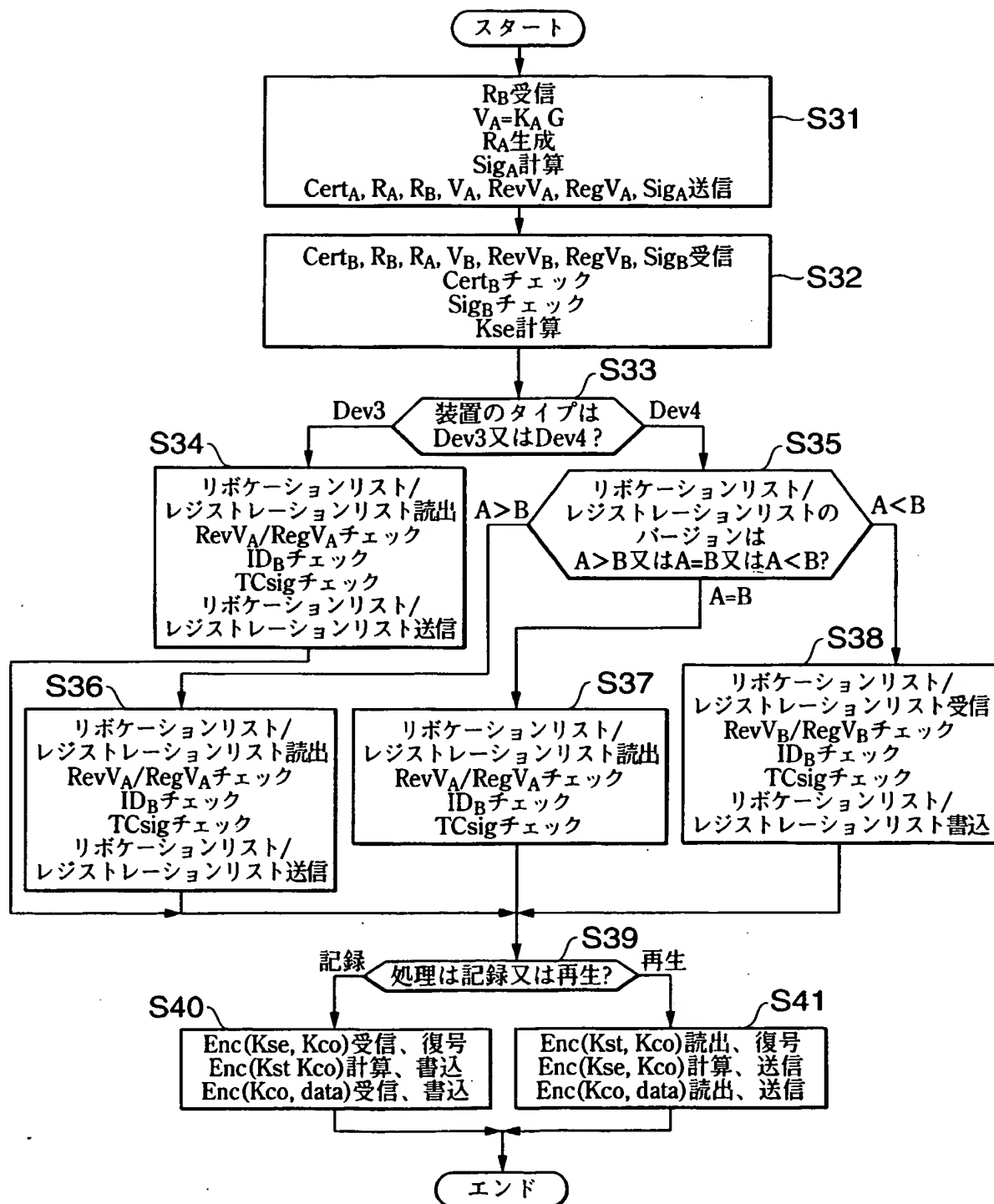


FIG.83

**THIS PAGE BLANK (USPTO)**

83/94

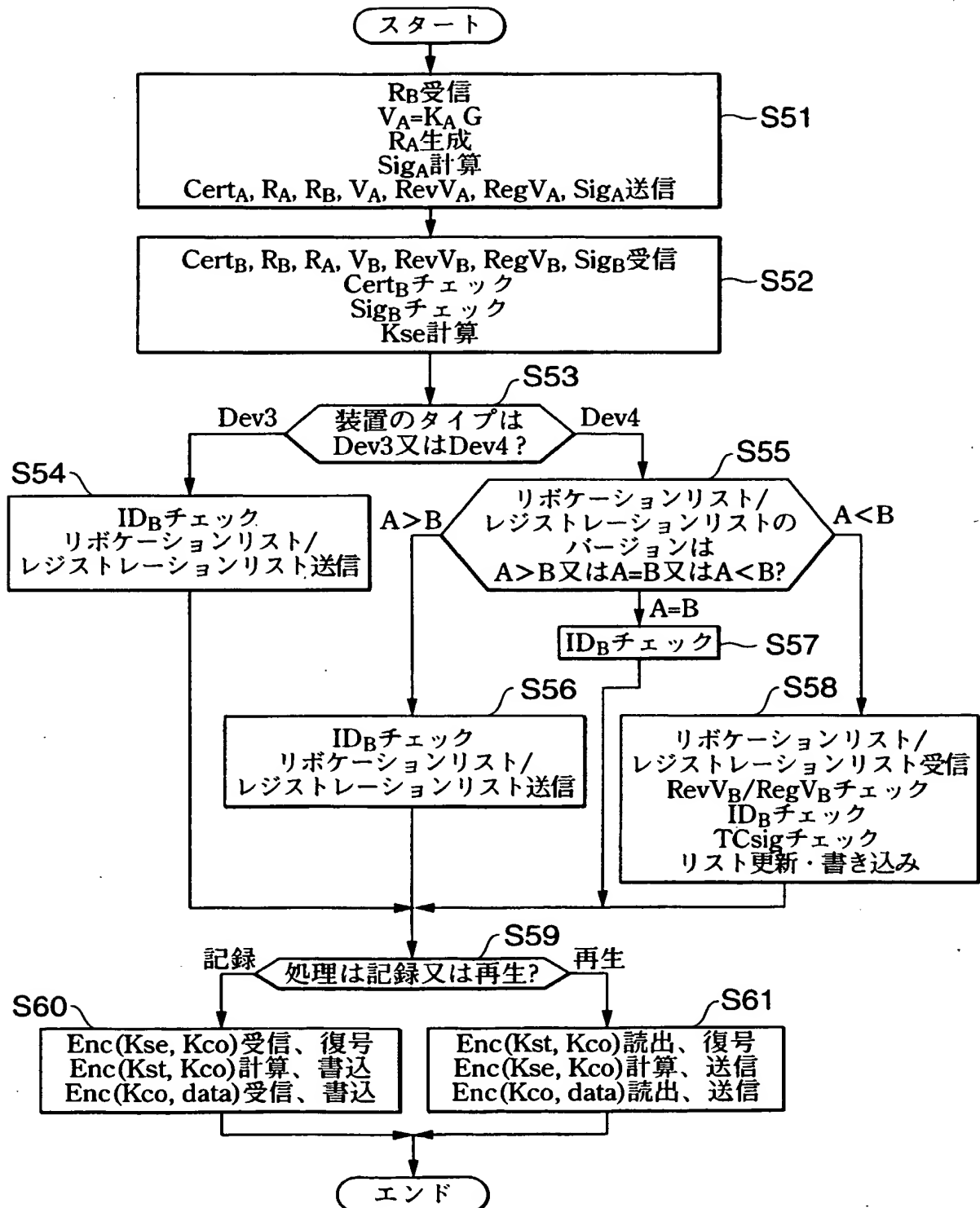


FIG.84

**THIS PAGE BLANK (USPTO)**



84/94

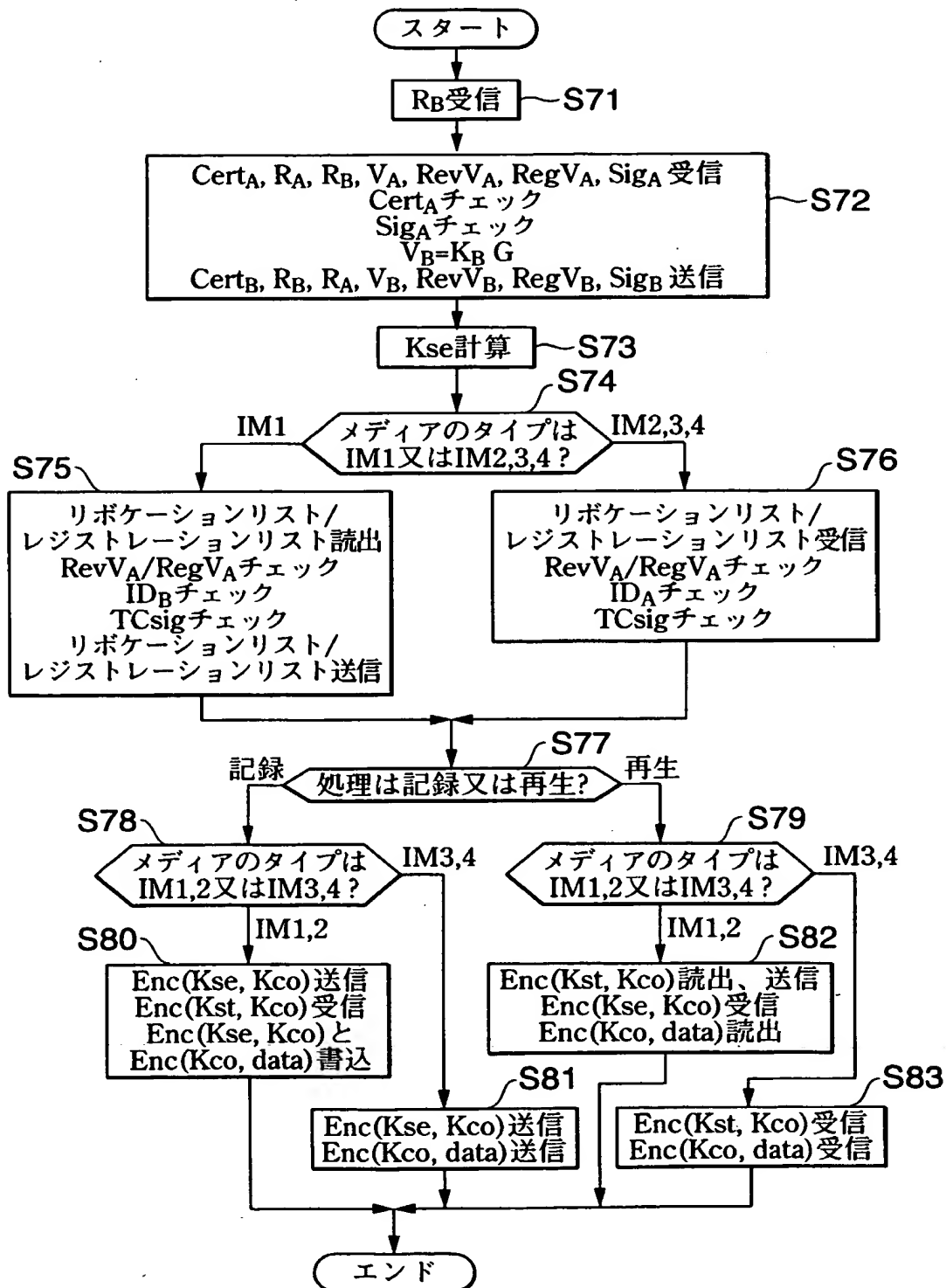


FIG.85

**THIS PAGE BLANK (USPTO)**

85/94

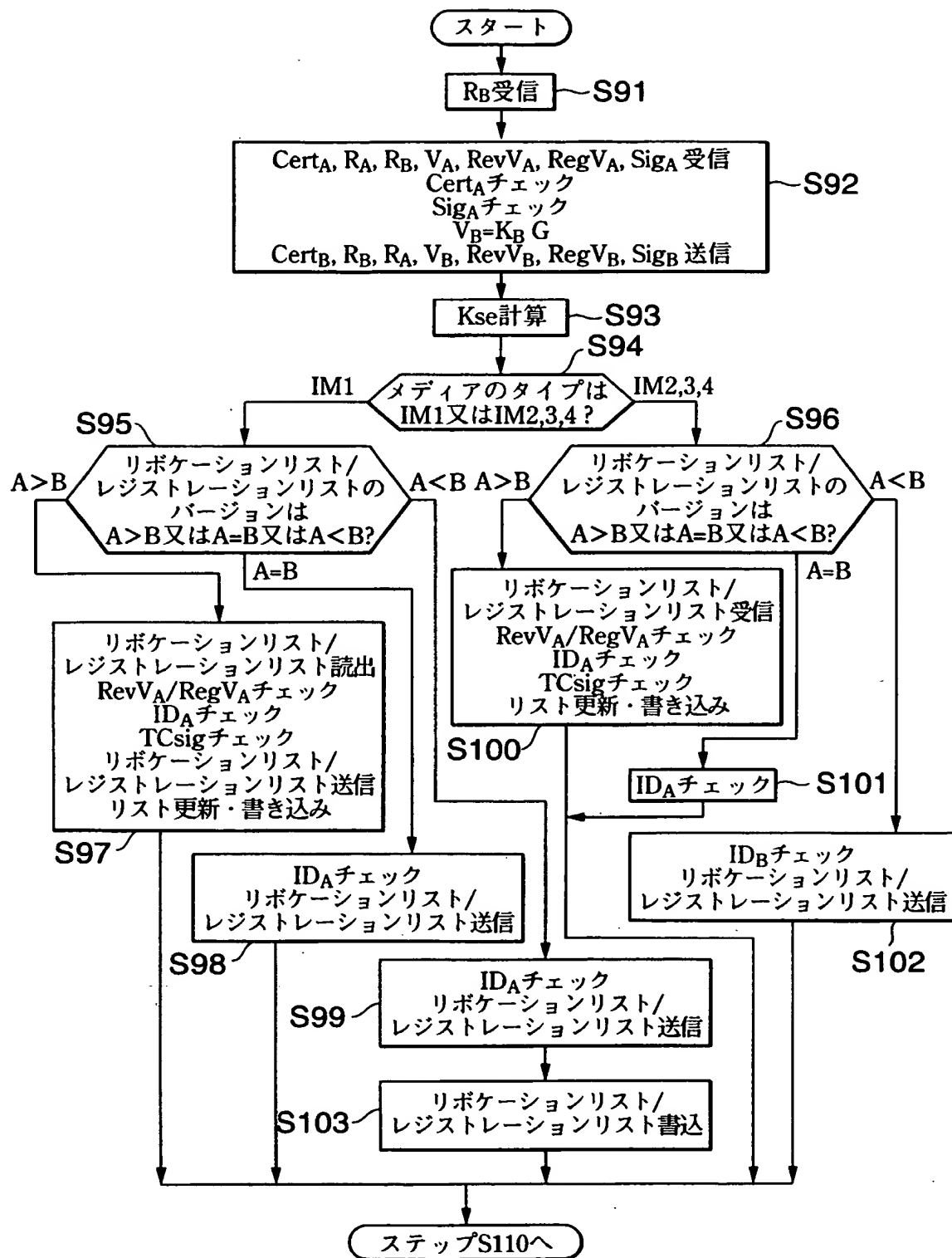


FIG.86

**THIS PAGE BLANK (USPTO)**

86/94

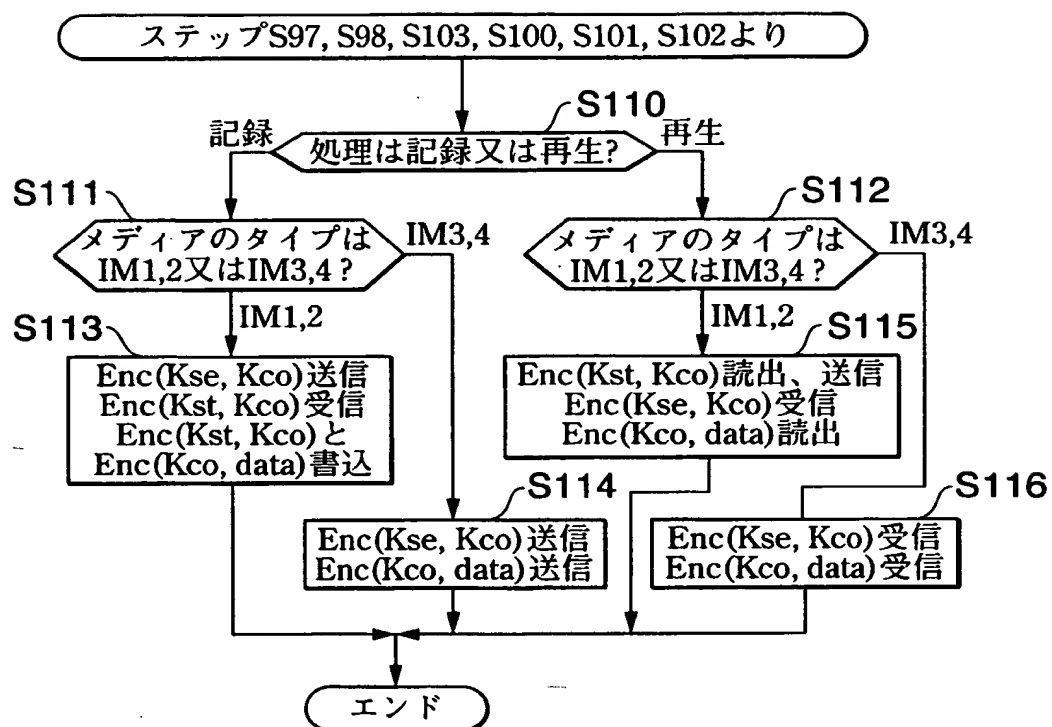


FIG.87

**THIS PAGE BLANK (USPTO)**

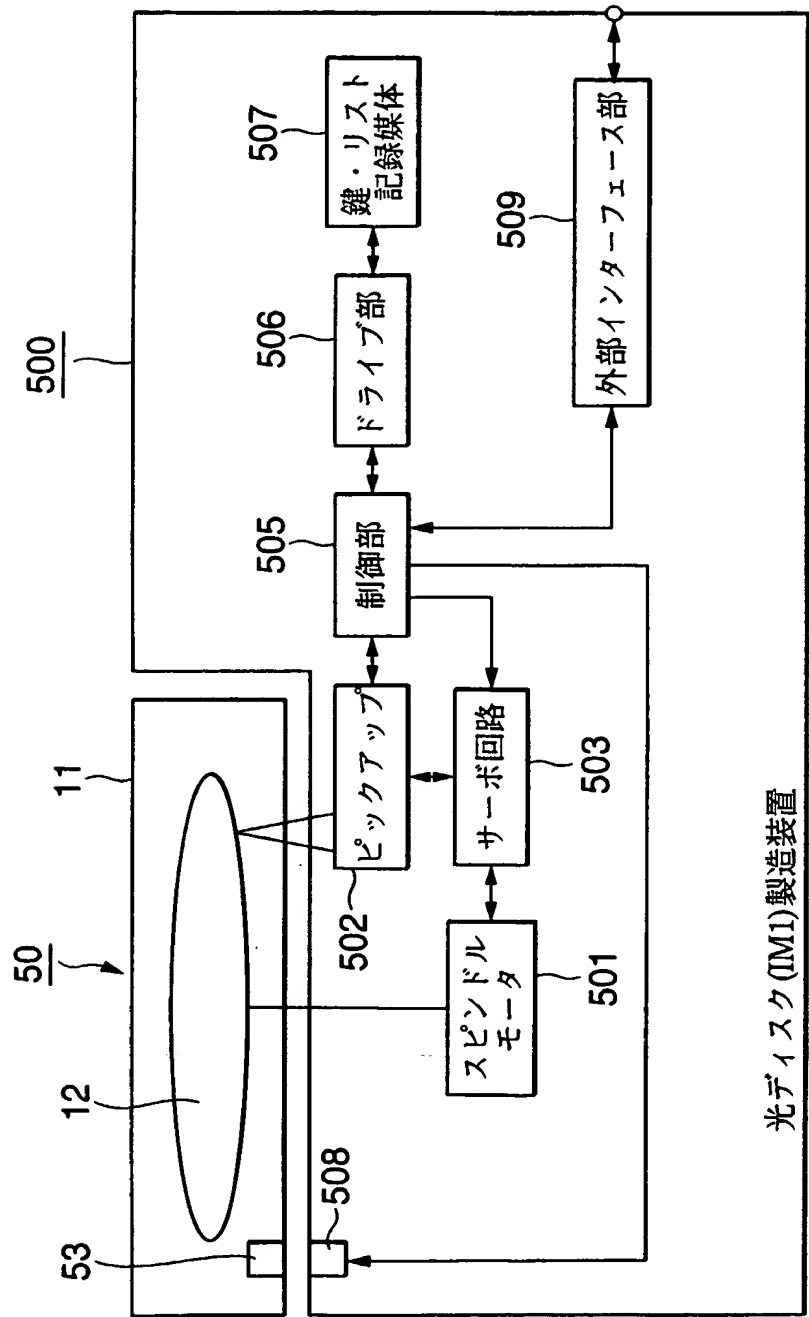


FIG.88

**THIS PAGE BLANK (USPTO)**



88/94

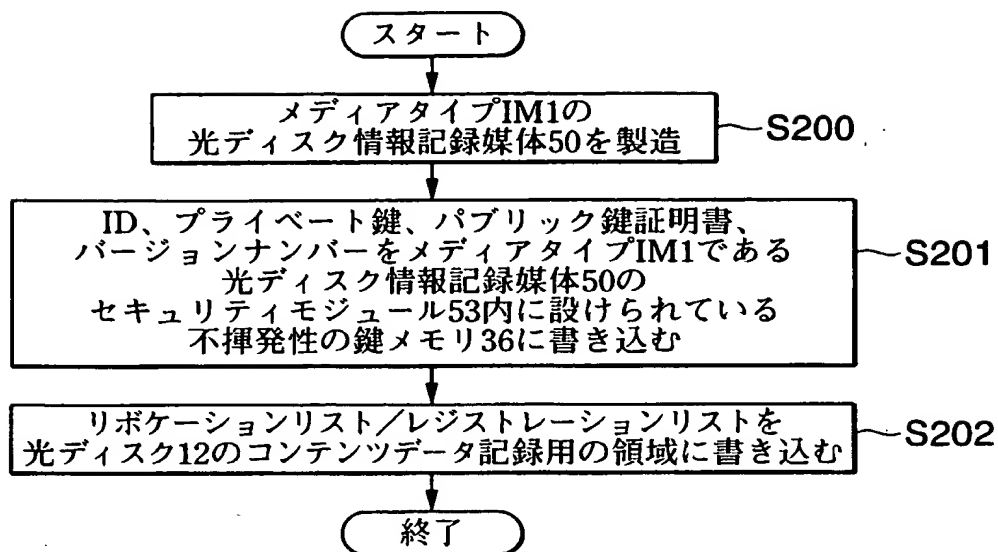


FIG.89

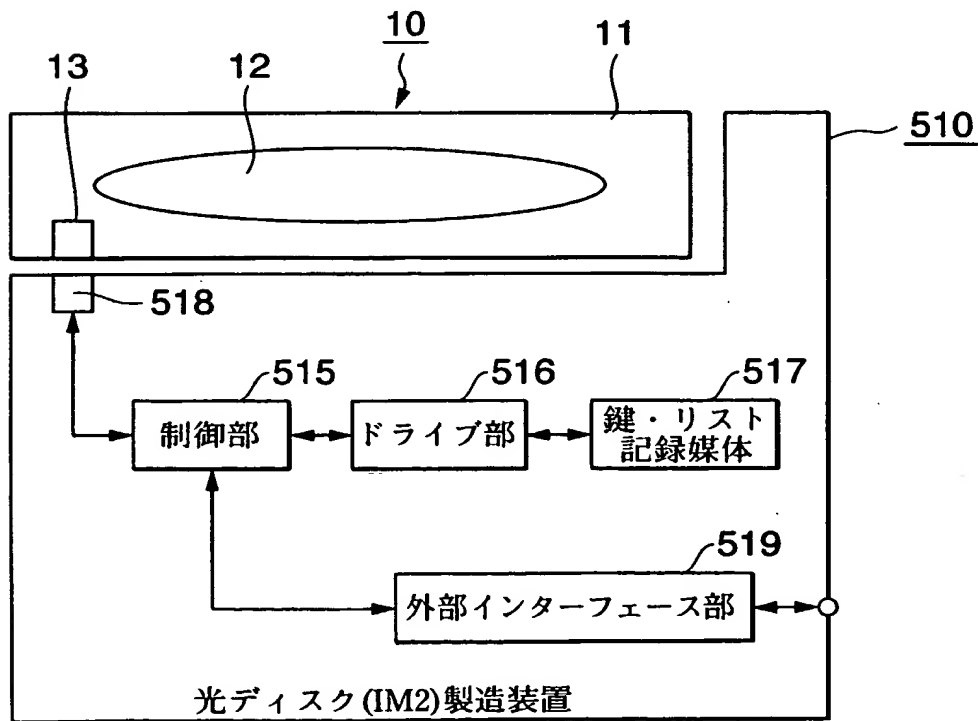


FIG.90

**THIS PAGE BLANK (USPTO)**

89/94

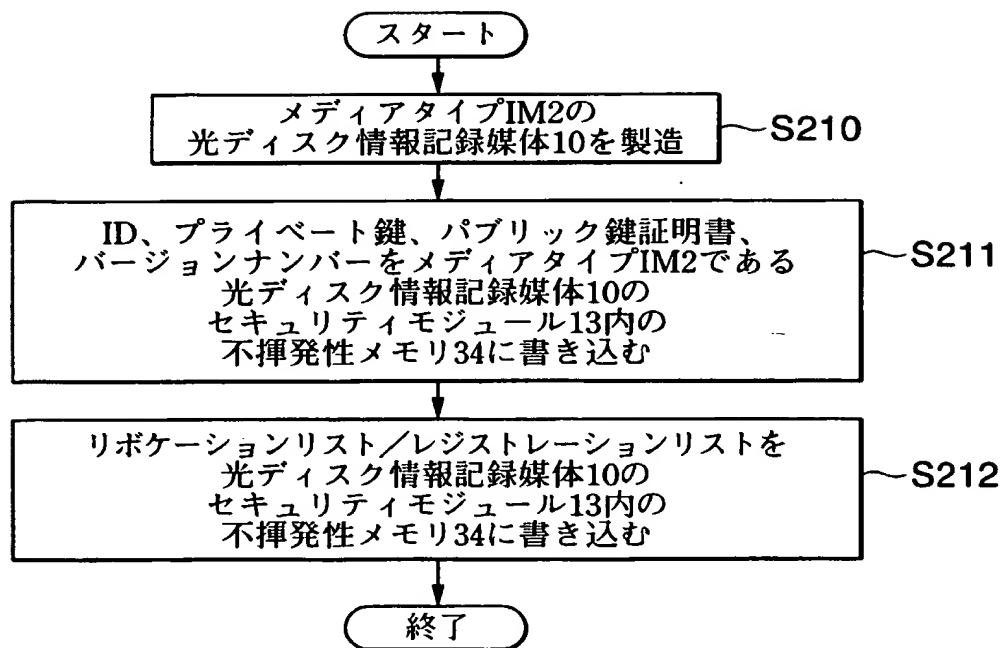


FIG.91

**THIS PAGE BLANK (USPTO)**

90/94

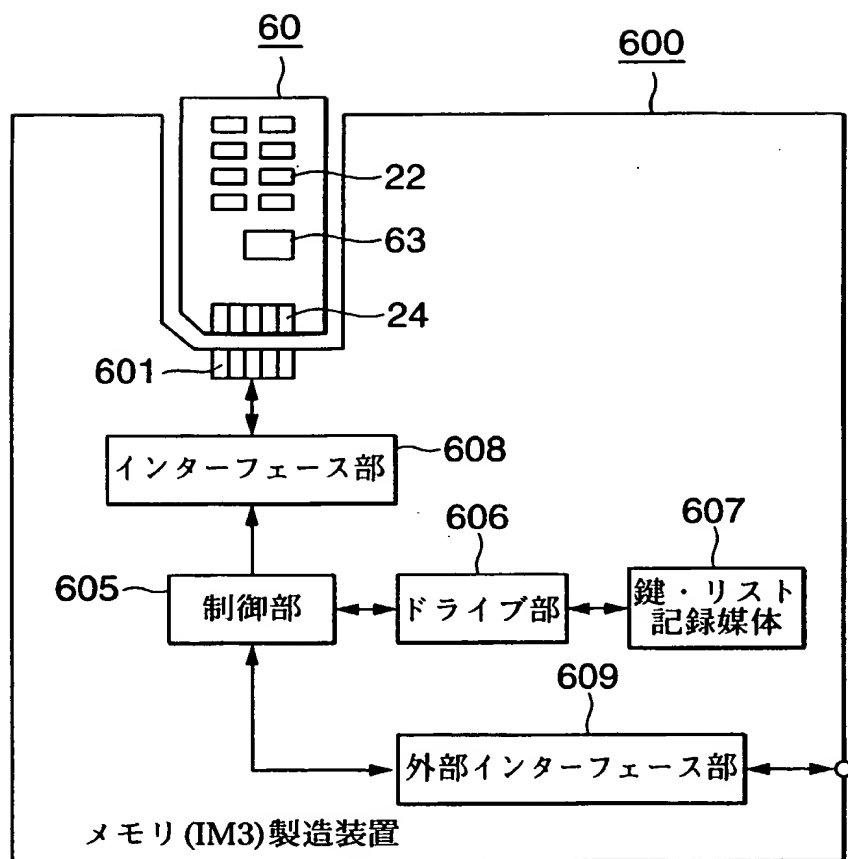


FIG.92

**THIS PAGE BLANK (USPTO)**

91/94

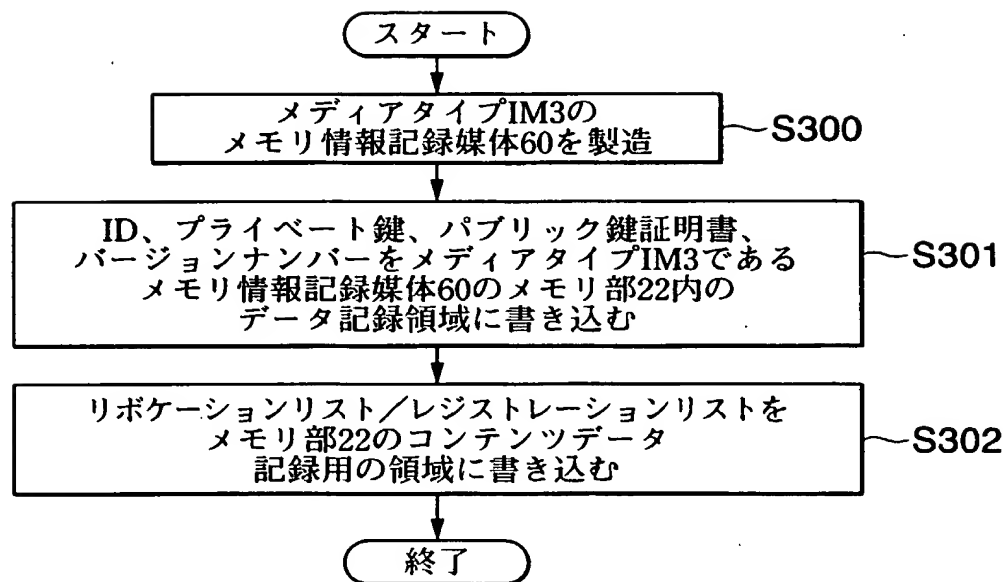


FIG.93

**THIS PAGE BLANK (USPTO)**



92/94

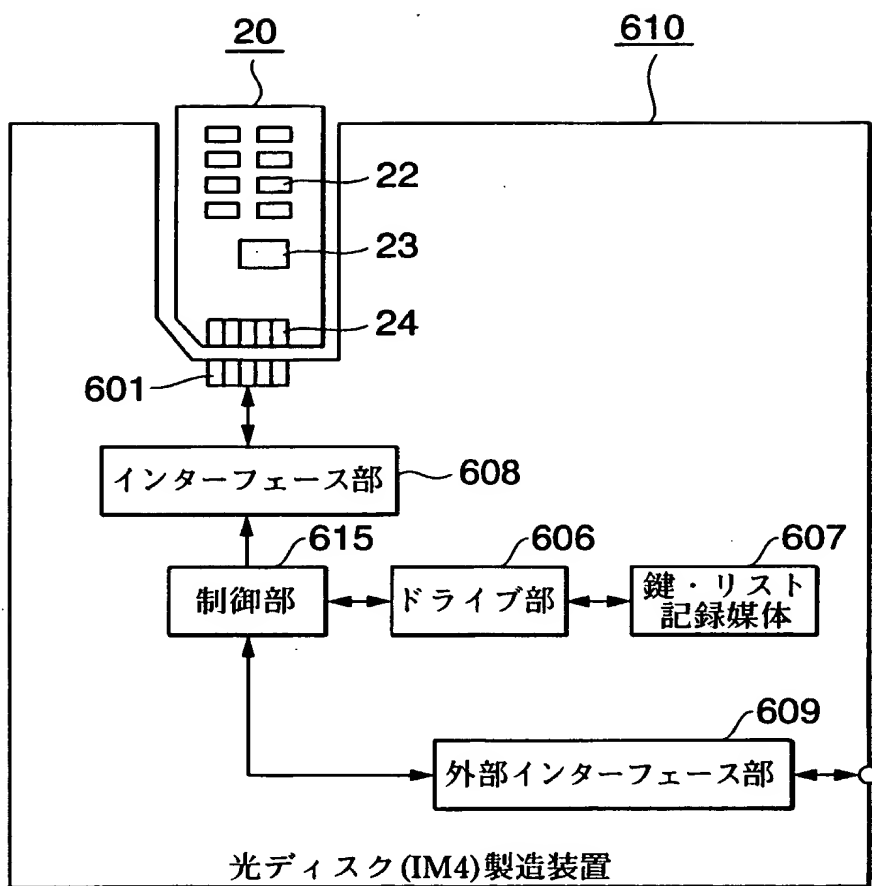


FIG.94

**THIS PAGE BLANK (USPTO)**

93/94

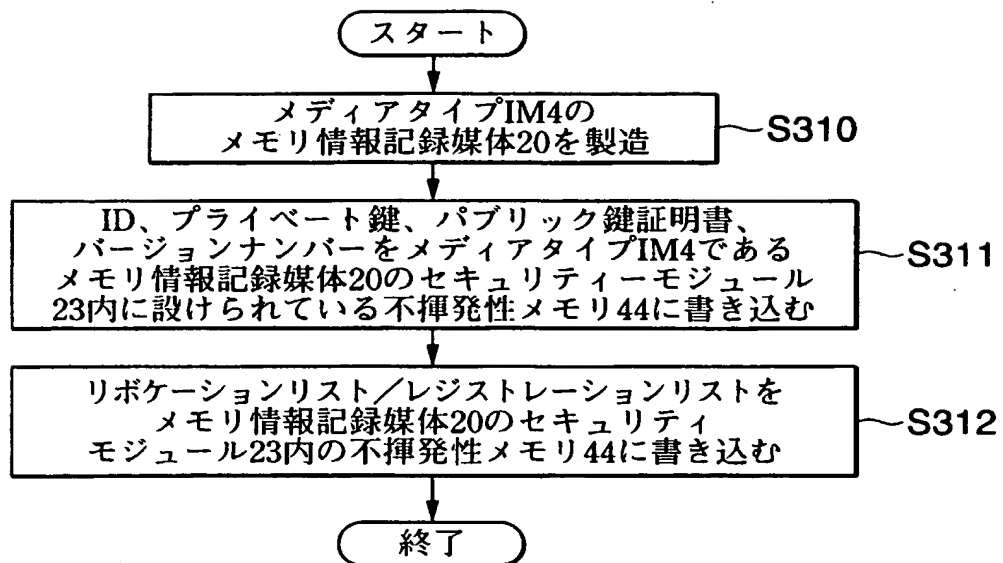


FIG.95

**THIS PAGE BLANK (USPTO)**

94/94

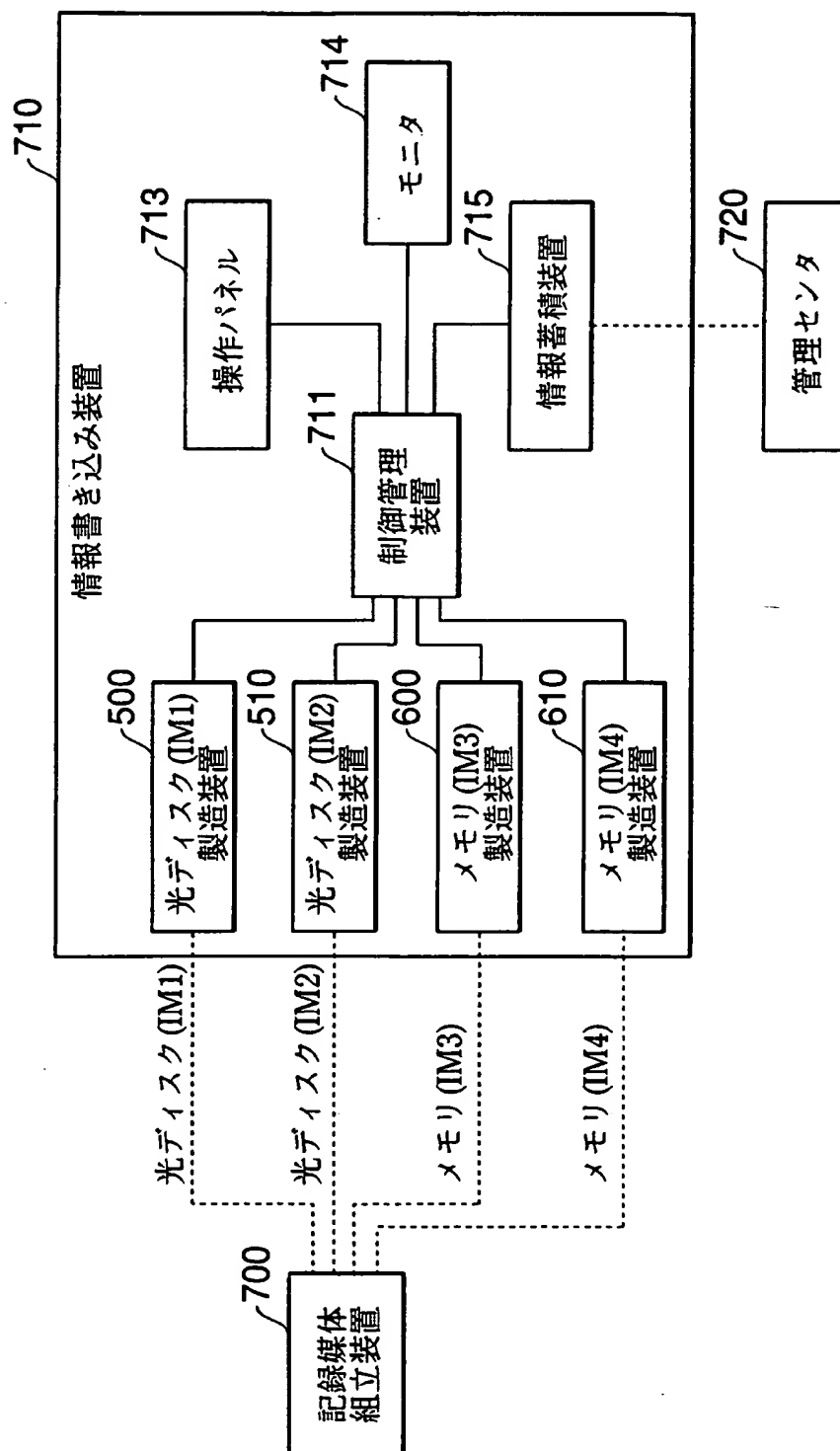


FIG.96

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L 9/32 H04L 9/08 G11B 20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L 9/00 G09C 1/00-5/00 G11B 20/00 G06K 17/00  
G06F 12/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS)

INSPEC (WPI)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Taro YOSHIO, "Kogata Memory Card de Ongaku Chosakuken wo mamoru," Nikkei Electronics, 22 March, 1999 (22.03.99) (Np.738), pp.49-53, especially, see page 51, middle column, and Fig. 1	1, 2, 6, 7, 34, 35, 37, 64, 65, 67, 69, 91-93, 95
Y		3-5, 21-23, 26-33, 36, 51-53, 56-63, 66, 68, 78-80, 83-90, 94, 102-104, 107-117
A		1-137
X	JP, 10-133953, A (TOKIMEC INC.), 22 May, 1998 (22.05.98) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	JP, 5-75598, A (Matsushita Electric Ind. Co., Ltd.), 26 March, 1993 (26.03.93) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:  
 "A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier document but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
26 October, 2000 (26.10.00)Date of mailing of the international search report  
07 November, 2000 (07.11.00)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 63-184164, A (Hikari YOKOEKAWA), 29 July, 1988 (29.07.88) (Family: none)	1, 6, 34, 64, 67, 91, 93
Y		115-117
Y	JP, 11-7412, A (Oputoromu K.K.), 12 January, 1999 (12.01.99) & WO, 98/58319, A1 & EP, 919929, A1 & AU, 9880344, A & CN, 1229487, A & TW, 374912, A	3-5, 36, 66, 68, 94
Y	JP, 7-161172, A (Sony Corporation), 23 June, 1995 (23.06.95) (Family: none)	3-5, 36, 66, 68, 94
Y	JP, 11-120679, A (Sony Corporation of America), 30 April, 1999 (30.04.99) (Family: none)	3-5, 36, 66, 68, 94
Y	Naoji USUKI, et al., "IEEE1394 Bus no Chosakuken Hogo Houshiki", Eizou Jouhou Media Gakkai Gijutsu Houkoku, Vol.22, No.65, (Nov 1998), pp.37-42 (CE'98-14), especially, see page 38, left column	26, 28-30, 32, 56 , 58-60, 62, 83, 8 5-87, 89, 107, 10 9-111, 113
Y	Katsuichi HIROSE, et al., "Anzena Ninshoutsuki Diffie-Hellman Kagi Kyoyuu Protocol to sono Kaigi Kagi Haifu eno Ouyou", Technical Research report, the Institute of Electronics, Information and Communication Engineers, Vol.97, No.252, (1997), pp.87-96 (ISEC97-37)	27, 31, 33, 57, 61 , 63, 84, 88, 90, 1 08, 112, 114
Y	JP, 5-347617, A (Toshiba Corporation), 27 December, 1993 (27.12.93) (Family: none)	27, 31, 33, 57, 61 , 63, 84, 88, 90, 1 08, 112, 114
Y	Rainer A Rueppel and Paul G van Oortscot, "Modern key agreement techniques," computer communications, (July, 1994), pp.458-465	115-117  8-25, 38-55, 70-82, 96-106
Y	Lein Harn and Shoubao Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution," IEEE Journal on Selected Areas in Communications, Vol.11, No.5, (June, 1993), pp.757-760	115-117  8-25, 38-55, 70- 82, 96-106
Y	JP, 2-278489, A (CSK Corporation), 14 November, 1990 (14.11.90) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38-50, 54, 55, 70-77, 81-82, 96-101, 105, 106 , 118-137
Y	JP, 10-187826, A (NEC Corporation), 21 July, 1998 (21.07.98) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38- 50, 54, 55, 70-77 , 81, 82, 96-101, 105, 106, 118-13 7



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 7-319967, A (TEC CORPORATION), 08 December, 1995 (08.12.95) (Family: none)	21-23, 51-53, 78-80, 102-104
A		8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
A	JP, 11-205305, A (Sony Corporation), 30 July, 1999 (30.07.99) & EP, 930556, A2	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
A	JP, 6-161354, A (Nippon Telegr. & Teleph. Corp. <NTT>), 07 June, 1994 (07.06.94) & EP, 856821, A2 & EP, 856822, A2 & US, 5396558, A & US, 5446796, A & US, 5502765, A	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106 , 118-137
Y	Digital Transmission Content Protection Specification, Revision 1.0, (12 Apr 1999), Volume 1 (Informational Version), Especially, see Chapter 4, Par. No. 4.5 and Chapter 7	2, 8-13, 17-23, 35, 38-43, 47-53 , 65, 70-72, 75-80, 92, 96, 99-104, 115-137

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05543

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

Claims 1 to 117 relate to a system consisting of a drive device and an information recording medium that mutually authenticate each other, or individual devices, or a method of information transmission between individual devices or a method of accessing an information recording medium, while claims 118 to 137 relate to a recording medium production device or a recording medium production method.

Although the both (group of claims 1 to 117 and group of claims 118 to 137) share only a recording medium and an information recording medium including a security module for mutual authenticating, our search result has evidenced that the mutually-authenticating information recording medium is disclosed in "Protecting music copyright by small-sized memory card" by Taro Yoshio, Nikkei Electronics, No. 739 (1999-3-22), pp.49-53, and therefore is not novel.

Accordingly, since the subject matters shared by the group of claims 1 to 117 and the group of claims 118 to 137 are still at a prior-art level, they do not constitute any special technical matters in terms of the second sentence of PCT Rule 13.2. Therefore, the above two groups of claims do not fulfill the requirement of unity of invention.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup>

H04L 9/32 H04L 9/08 G11B 20/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup>H04L 9/00 G09C 1/00-5/00 G11B 20/00 G06K 17/00  
G06F 12/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

INSPEC (WPI)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	芳尾太郎 “小型メモリ・カードで音楽著作権を守る” 日経エレクトロニクス, 1999年3月22日号 (No. 738), pp. 49-53, 特に51頁中欄及び図1参照	1, 2, 6, 7, 34, 35, 37, 64, 65, 67, 69, 91-93, 95
Y		3-5, 21-23, 26-33, 36, 51-53, 56-63, 66, 68, 7 8-80, 83-90, 94, 102- 104, 107-117
A		1-137

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

26. 10. 00

国際調査報告の発送日

07.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

丸山 高政

5W

9570

電話番号 03-3581-1101 内線 3576

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 10-133953, A (株式会社トキメック) 22. 5月. 1998 (22. 05. 98), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	J P, 5-75598, A (松下電器産業株式会社) 26. 3月. 1993 (26. 03. 93), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
X	J P, 63-184164, A (横江川 光) 29. 7月. 1988 (29. 07. 88), ファミリーなし	1, 6, 34, 64, 67, 91, 93
Y		115-117
Y	J P, 11-7412, A (株式会社オプトロム) 12. 1月. 1999 (12. 01. 99) &WO, 98/58319, A1 &EP, 919929, A1 &AU, 9880344, A &CN, 1229487, A &TW, 374912, A	3-5, 36, 66, 68, 94
Y	J P, 7-161172, A (ソニー株式会社) 23. 6月. 1995 (23. 06. 95), ファミリーなし	3-5, 36, 66, 68, 94
Y	J P, 11-120679, A (ソニー コーポレーション オブ アメリカ) 30. 4月. 1999 (30. 04. 99), ファミリーなし	3-5, 36, 66, 68, 94
Y	臼木直司, 飯塚裕之, 山田正純, 松崎なつめ “IEEE1394バスの著作権保護方式”, 映像情報メディア学会技術報告, Vol. 22, No. 65, (Nov 1998), pp. 37-42 (CE'98-14), 特に38頁左欄参照	26, 28-30, 32, 56, 58-60, 62, 83, 85-87, 89, 107, 109-111, 113
Y	廣瀬勝一, 吉田進 “安全な認証付Diffie-Hellman鍵共有プロトコル とその会議鍵配布への応用”, 電子情報通信学会技術研究報告, Vol. 97, No. 252, (1997), pp. 87-96 (ISEC97-37)	27, 31, 33, 57, 61, 63, 84, 88, 90, 108, 112, 114
Y	J P, 5-347617, A (株式会社東芝) 27. 12月. 1993 (27. 12. 93), ファミリーなし	27, 31, 33, 57, 61, 63, 84, 88, 90, 108, 112, 114

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	Rainer A Rueppel and Paul G van Oorschot, "Modern key agreement techniques," computer communications, (Jul 1994), pp. 458-465	115-117 8-25, 38-55, 70-82, 96-106
Y A	Lein Harn and Shoubao Yang, "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution," IEEE Journal on Selected Areas in Communications, Vol.11, No.5, (Jun 1993), pp. 757-760	115-117 8-25, 38-55, 70-82, 96-106
Y A	J P, 2-278489, A (株式会社シーエスケイ) 14. 11月. 1990 (14. 11. 90), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y A	J P, 10-187826, A (日本電気株式会社) 21. 7月. 1998 (21. 07. 98), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y A	J P, 7-319967, A (株式会社テック) 8. 12月. 1995 (08. 12. 95), ファミリーなし	21-23, 51-53, 78-80, 102- 104 8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
A	J P, 11-205305, A (ソニー株式会社) 30. 7月. 1999 (30. 07. 99) &EP, 930556, A2	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	J P, 6-161354, A (日本電信電話株式会社) 7. 6月. 1994 (07. 06. 94) &EP, 856821, A2 &EP, 856822, A2 &US, 5396558, A &US, 5446796, A &US, 5502765, A	8-20, 24, 25, 38-50, 54, 55, 70-77, 81, 82, 96-101, 105, 106, 118-137
Y	Digital Transmission Content Protection Specification, Revision 1.0, (12 Apr 1999), Volume 1 (Informational Version), 特に第4章4.5節及び第7章参照	2, 8-13, 17- 23, 35, 38-43, 47-53, 65, 70- 72, 75-80, 92, 96, 99-104, 115-137

## 第I欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第II欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲1-117は、相互認証を行うドライブ装置及び情報記録媒体からなるシステム、あるいは各々の装置、あるいは各々の装置間での情報伝達方法又は情報記録媒体へのアクセス方法に関するものであり、一方、請求の範囲118-137は、記録媒体製造装置又は記録媒体製造方法に関するものである。

この両者(請求の範囲1-117の群と請求の範囲118-137の群)に共通の事項は、記録媒体及び相互認証のためのセキュリティモジュールを含む情報記録媒体のみであるが、調査の結果、相互認証を行う情報記録媒体は、芳尾太郎“小型メモリ・カードで音楽著作権を守る”日経エレクトロニクス、第739号、(1999年3月22日)、pp. 49-53に開示されているから、新規でないことが明らかとなった。

結果として、請求の範囲1-117の群と請求の範囲118-137の群とに共通の事項は、先行技術の域を出ないから、PCT規則13.2の第2文の意味において、特別な技術的事項ではない。したがって、上記2群の請求項は、発明の単一性を満たしていない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

## 追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**